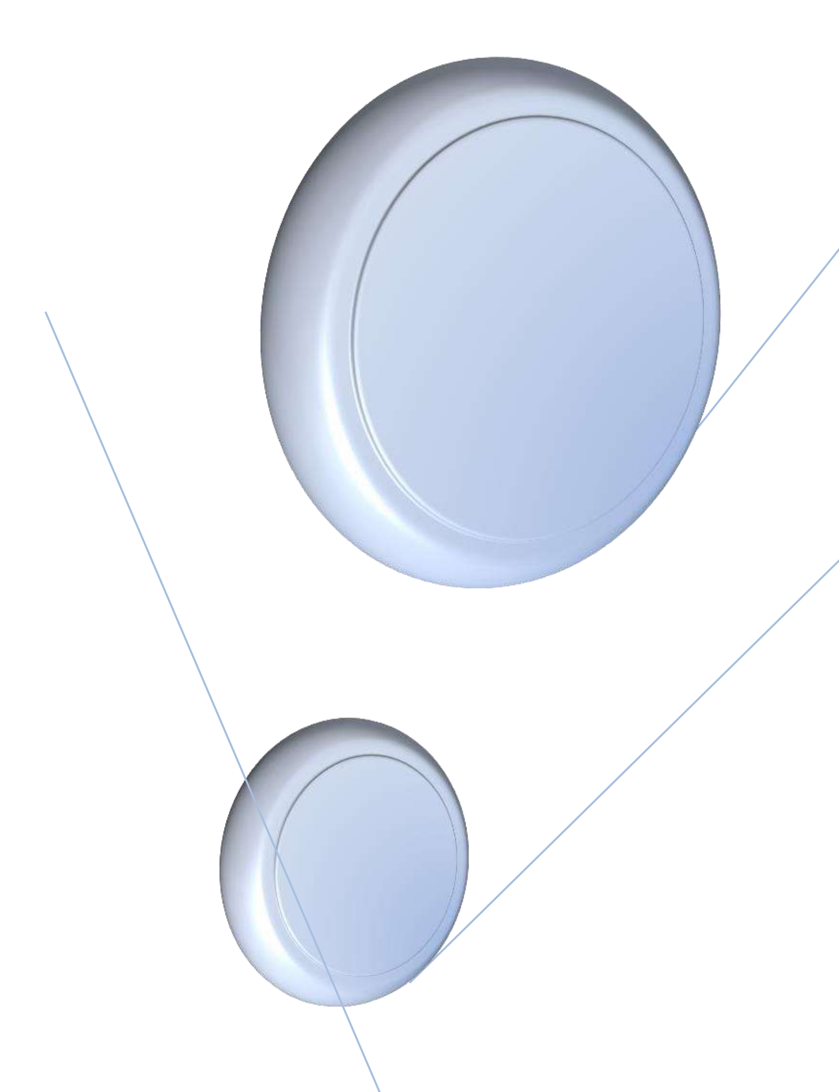
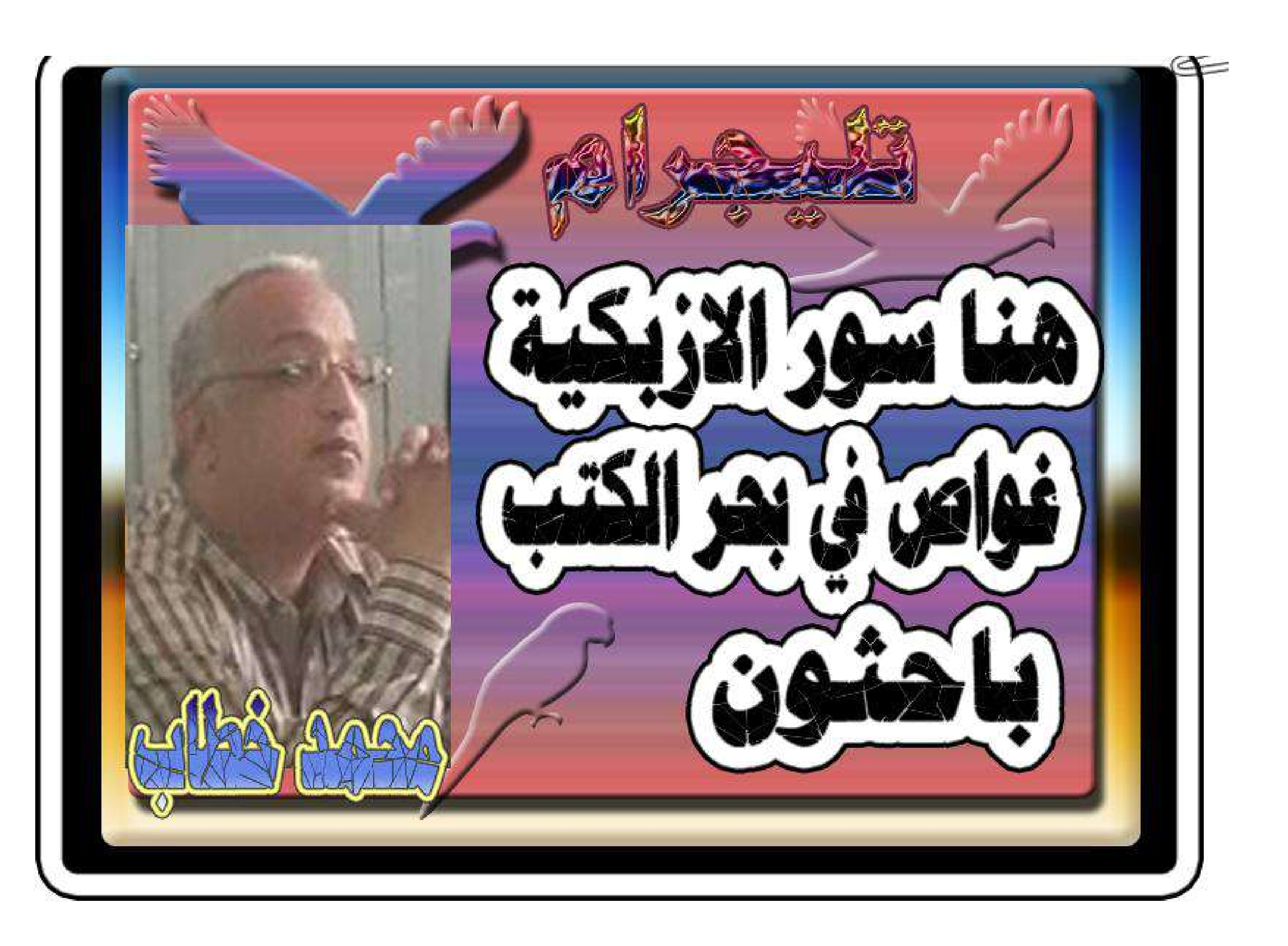


الأمن السيبراني ودوره في حماية الأمن القومي



امراجع عطية السحاتي

الأمن السيبراني ودوره في حماية الأمن القومي



أمراجع عطية السحاتي

ملخص الدراسة

تحاول هذه الدراسة ابراز دور الأمن السيبراني في حماية الأمن القومي للدول وأهم التحديات التي تواجهه في ظل التطور السريع في وسائل الاتصال الإلكتروني عبر شبكات الإنترنت ، كما تحاول إيجاد معالجات وحلول لهذه التحديات وذلك من خلال الإجابة على التساؤل الذي يقول :- ما دور الأمن السيبراني في حماية الأمن القومي للدول ؟ وكان الهدف منها ابراز دور الأمن السيبراني في حماية الأمن القومي للدول ، وابراز أهم التحديات والصعوبات التي توجهه وأهم الحلول والمعالجات لتحقيقه ، وتأتي اهميتها لكونها توضح دور الأمن السيبراني في حماية الأمن القومي وابراز أهم التحديات التي تواجهه وأهم الحلول والمعالجات لتحقيقه ، اما منهج الدراسة فهو منهج دراسة الحالة ، وكانت أهم نتائج الدراسة إن للأمن السيبراني دور في حماية الأمن القومي للدول وهو جزء منه ، هذا وقد كانت أهم التوصيات ضرورة نشر الوعي بالأمن السيبراني ووقاية وحماية شبكات وتطبيقات وبرمجيات واجهزة الدولة الإلكترونية من أي هجمات سيبرانية .

<u>الكلمات المفتاحية :-</u>

الأمن . السيبراني . دوره . الحماية . الأمن القومي .

Study summary

This study attempts to highlight the role of cybersecurity in protecting the national security of countries and the most important challenges facing it in light of the rapid development of means of electronic communication via Internet networks. It also attempts to find solutions to these challenges by answering the question that says: - What is the role of cybersecurity in Protecting the national security of countries? Its aim was to highlight the role of cybersecurity in protecting the national security of countries. It highlights the most important challenges and difficulties that guide it and the most important solutions and treatments to achieve it. Its importance comes because it explains the role of cybersecurity in protecting national security and highlighting the most important challenges facing it and the most important solutions and treatments to achieve it. The study methodology is the case study approach. The most important results of the study were that cybersecurity has a role in protecting the national security of countries and is part of it. The most important recommendations were the necessity of spreading awareness of cybersecurity and preventing and protecting the state's electronic networks, applications, software and devices from any cyber attacks.

key words :-

Security . Cyber. turn . Protection. National Security .

مقدمة

صار الامر ملحاً لوجود أمن سيبراني مع التطور في وسائل الاتصال عبر الإنترنت والتي بالإمكان اختراقها من أي جهة خاصة وان العالم بما فيه من مؤسسات خاصة وعامة وافراد صارت تعتمد على هذا النوع من الاتصال والاطلاع والارشفة حيث صارت تحفظ ملفات وسجلات سياسية وعسكرية واقتصادية وثقافية واجتماعية وبيئية ذات خصوصية حساسة وصارت معلومات وبيانات وتطبيقات جوانب الأمن القومي التي يعنى بحمايتها الأمن القومي في الفضاء السيبراني فعدم تأمينها سيبرانياً يعرضها للسرقة والتدمير والاختراق والتشفير وبهذا فان ذلك سوف يهدد الامن القومي ووجود الأمن السيبراني لحماية تلك المحتويات من انظمة وبيانات وشبكات وبرامج إلكترونية سوف يحمي كافة جوانب الأمن القومي وفروعها المختلفة ، وليبيا من احد الدول التي تهددها الهجمات السيبرانية وتحتاج الى أمن سيبراني يساهم في حماية ووقاية كافة جوانب أمنها القومي وفروعها المختلفة لما لهذا الأمن من دور في حماية الأمن القومي في ظل التطور السريع في وسائل الاتصال الإلكتروني . ظهر مفهوم الأمن السيبراني لأول مرة في عام 1972م ، ومع تقدم التكنولوجيا وازدياد التطور في وسائل الاتصال المختلفة وبعد ان اعتمدت الدول حكومات وافراد على الفضاء الرقمي عبر الشبكة الدولية للمعلومات الإنترنت وصارت هناك اختراقات

لخصوصيات الدول والافراد صار من الضروري ان يكون هناك حل لهذه الخروقات التي صارت تهدد الأمن القومي للدول فلهذا كان الأمن السيبراني .

تحاول هذه الدراسة ابراز اهم التحديات التي تواجه تحقيق الأمن السيبراني في ظل التطور السريع في وسائل الاتصال الإلكتروني واعتماد المؤسسات والافراد على الارشفة الإلكترونية دون سواها ، كما تحاول إيجاد حلول ومعالجات لهذه التحديات ، كما تحاول ابراز دور الأمن السيبراني في حماية الأمن القومي ، وذلك من خلال الإجابة على التساؤل الذي يقول :- ما دور الأمن السيبراني في حماية الأمن القومي لدولة ما ؟ ، اما منهج الدراسة فهو منهج دراسة الحالة ، هذا وكان الاطار المنهجي لهذه الدراسة كالاتي :-

أ- مشكلة الدراسة :

تمثلت مشكلة الدراسة في التحديات التي تواجه تحقيق الأمن السيبراني والتي تؤثر على الأمن القومي لدولة ما ، وتقوم إشكالية الدراسة على تساؤل يقول : ما دور الأمن السيبراني في حماية الأمن القومي لدولة ما ؟

ب- أهمية الدراسة :

1- إيجاد حلول ومقترحات للتحديات التي تواجه تحقيق الأمن السيبراني .

2- ابراز دور الأمن السيبراني في حماية على الأمن القومي .

3- المساهمة في تعزيز حماية الأمن السيبراني .

4- التعريف بأهمية الأمن السيبراني في حماية الأمن القومي .

ت- أهداف الدراسة :

لقد تمثلت أهداف الدراسة في الأهداف التالية :-

1- تحديد أهم التحديات التي تواجه تحقيق الأمن السيبراني وكيفية القضاء عليها .

2- تعزيز الدراسات في مجال الأمن السيبراني والتعريف به .

3- ابراز دور الأمن السيبراني في حماية الأمن القومي .

4- إثراء المكتبة الليبية بهذه الدراسة.

ج- منهج الدراسة :

استخدم في هذه الدراسة منهج دراسة حالة وهو منهج يحلل الدراسة ويركز على ظاهرتها عن طريق دراستها وتحليلها ، وهي التحديات التي تواجه تحقيق الأمن السيبراني ليؤدي دوره في حماية الأمن القومي .

ح- وسائل جمع البيانات والمعلومات :

كانت وسائل جمع البيانات والمعلومات من المصادر غير الميدانية خاصة المصادر الثانوية كالكتب

إضافة الى الشبكة الدولية للمعلومات "الإنترنت " .

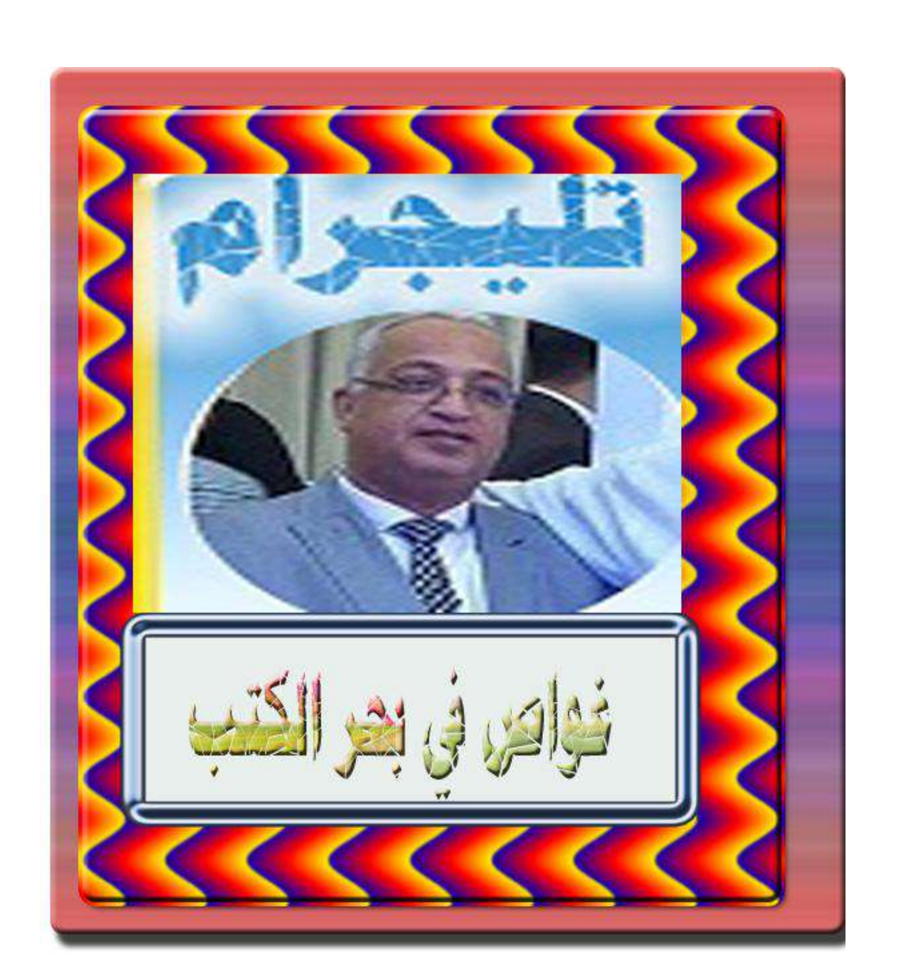
هذا وقد قسمت الدراسة إلى الاتي : –

أولاً : الأمن السيبراني (المفهوم . الأهداف .الأهمية . الأنواع .علاقته بالأمن القومي) .

ثانياً : ثانياً أهم التحديات التي تواجه الأمن السيبراني .

ثالثاً : أهم الحلول والمعالجات التي تعالج التحديات التي تواجه الأمن السيبراني .

رابعاً : النتائج والتوصيات.



أولاً الأمن السيبراني

(المفهوم . الأهمية. الأهداف . الأنواع . علاقته بالأمن القومي)

أ- مفهوم الأمن السيبراني :

هناك من يطلق عليه أمن الحاسوب وهناك من يطلق عليه الأمن الإلكتروني وهناك من اطلق عليه أمن المعلومات والذي يعرف بأنه "هو الذي يهتم بالحفاظ على مدى سرية المعلومات والبيانات التي يقوم مستخدم الإنترنت بربطها ببعض مواقع التواصل الاجتماعي والمنصات الإلكترونية من أي محاولة اختراق أو تجسس إلكتروني " .... ، وهناك من اشار الى انه أمن شبكات حيث قيل بانه " يعني (أمن الشبكات)" (1) .

وهناك من يشير بان أمن المعلومات شيء والأمن السيبراني شيء آخر حيث اشير بانه يوجد بينهما اختلاف فأمن المعلومات مثلاً يقوم بحفظ جميع بيانات المستخدم التي تعطى له عند الموافقة على شروط التطبيق الإلكتروني في حين الأمن السيبراني يقوم بمنع التجسس على التطبيق الإلكتروني والابتزاز من المستخدم ، وأشير كذلك بان أمن المعلومات يحفظ جميع البيانات عند الموافقة على شروط استخدام التطبيق الإلكتروني ، اما الأمن السيبراني فانه يمنع التطبيق ذاته من التجسس والابتزاز والتتبع والاهتمام

على منصات التطبيق ، ولكن مع التطور التكنولوجي والاتصالات والتطور في الدراسات والابحاث في مجال الأمن السيبراني صار لكل تسمية عناصرها واهدافها واهميتها الخاصة .الصراع فيه يكون في نطاق البيئة التقنية والهجمات تدار عن بعد من خلال برامج وتطبيقات مختلفة هدفها تدمير وسرقة واتلاف وتشفير وتعطيل بيانات ومعلومات الغير . هذا المفهوم يتكون من كلمتين هما الأمن والسيبراني ، فكلمة أمن فالمقصود بها باختصار هو الحماية من أي اخطار وتهديدات ، أما كلمة سيبراني فقد اشير بانها عبارة عن منظومة أو علم ظهر مع ظهور الاجهزة الإلكترونية المتطورة كأجهزة الحاسوب والهواتف الذكية وتطبيقاتها وغيرها من الاجهزة المرتبطة بالإنترنت (2) .

كما اشير بان كلمة (سايبر) مصطلح درج استخدامه لوصف الفضاء الذي يضم شبكات الاتصال والمعلومات وانظمة التحكم عن بعد (3) .

ظهر بظهور برنامج الزحف او سيبر(Creeper) الذي صممه الباحث والمصمم (روبرت توماس) ، وهذا البرنامج وكما اشير له القدرة على التحرك عبر شبكة تنيكس (4) .

كما اشير كذلك بان كلمة سايبر هي كلمة انجليزية وتعني كل ما له علاقة بالكمبيوتر والشبكة الدولية للمعلومات (الإنترنت) وتكنولوجيا المعلومات ، وهذا المصطلح كما اشير يشمل أنظمة التحكم عن بعد

كالبرمجيات الرقمية سوفت وير – الاجهزة الهارد وير – المبرمجين والمطورين ، واجهزة الكمبيوتر وتكنولوجيا المعلومات وغيرها من الاجهزة الحساسة ، وقد اشير بانه يتكون من ثلاثة اقسام وهي :-

1- البرمجيات الرقمية سوفت وير .

2- الاجهزة الهارد وير .

3- المبرمجين والمطورين(5) .

كما اشارت احد الدراسات كذلك بان كلمة سيبراني هو " نطاق افتراضي تم انشاؤه بواسطة اجهزة الحاسب الآلي المترابطة وشبكات الحاسب الآلي على الإنترنت " (6) .

وقيل كذلك بان السيبراني : " هو الوسط الذي تتواجد فيه جميع شبكات الحاسوب ويحصل من خلالها التواصل الإلكتروني "(7) .

إذن كلمة السيبراني تعني الفضاء الإلكتروني أي الفضاء السيبراني (Cyberspace) والذي عرف بأنه عبارة عن " بيئة تفاعلية رقمية تشمل عناصر مادية وغير مادية ، مكونة من مجموعة من الاجهزة الرقمية ، وانظمة الشبكات والبرمجيات ، والمستخدمين سواء مشغلين او مستعملين "(8) .

يعتبر الأمن السيبراني من تخصصات هندسة علوم الحساب وهو تخصص علمي كامل ، ظهر مع ظهور الاجهزة الإلكترونية التي تتصل بالشبكة الدولية للمعلومات (الإنترنت) وتطورها وما صار يهددها من

اختراقات تساهم في تهديد الأمن القومي بكافة جوانبه السياسية والعسكرية والثقافية والاجتماعية والاقتصادية وحتى البيئية وهو له دور في حماية الأمن القومي . مع التقدم في وسائل الاتصال الإلكترونية المرتبطة بالشبكة الدولية للمعلومات (الإنترنت) بدأت الحروب السيبرانية فقد صارت هناك هجمات من قبل دول وأفراد ضد دول وافراد من خلال هجمات سيبرانية على مواقع محددة وقد شملت تلك الهجمات شبكات التواصل الاجتماعي من فيس بوك وتويتر ورديت وتمبلر وغيرها ، وكذلك شبكات التواصل الفوري كالواتساب وتيلجرام والانستقرام وغيرها ، ولهذا كان من الضروري أن تكون هناك وسيلة للدفاع وصد تلك الهجمات ، لذلك ظهر الأمن الذي يحمي الفضاء السيبراني وهو المتمثل في الأمن السيبراني .

بمعنى ان مهمة أو وظيفة الأمن السيبراني هو حماية الاجهزة الإلكترونية بما فيها والمرتبطة بالإنترنت من أي اختراقات خارجية ، هناك من يقول حماية اجهزة الدولة الإلكترونية من أي هجوم سيبراني إلا ان الحقيقة هو حماية اجهزة الدولة والافراد وليس الدولة فقط فالأمن السيبراني هو أمن شامل ، والهجوم السيبراني (CyberAttack) هذا هو هجوم يهدف الى تعطيل وسرقة وابتزاز وتشفير البيانات والمعلومات ، وتدمير الاجهزة الإلكترونية لدولة ما من قبل دولة اخرى لغرض شل حركة نموها العسكري والاقتصادي والسياسي والاجتماعي والثقافي والبيئي . وهذا الهجوم حقيقة لا يستثني افراد او مؤسسات عامة او

خاصة ، وهو يؤدي الى خسارة في العديد من جوانب الأمن القومي وفروعها المختلفة فهو يضر بالصعيد المالي والاجتماعي والنفسي والشخصي ، والقصد منه طبعاً هو تعطيل وتدمير وسرقة ما يمكن ان يدمر ويسرق من انظمة معلومات الحواسيب الحساسة وشبكات (الإنترنت) وهو يهدد الأمن القومي للدولة(9) .

بسبب الزيادة في استخدام الإنترنت والاجهزة الإلكترونية بكثرة ظهرت هجمات من القرصنة والابتزاز الإلكتروني وصارت تهدد المستخدمين واجهزتهم ، وهذا هدد الأمن القومي وصار من الضروري التفكير في سياسات وطرق أمنية للتصدي لتلك الهجمات. لهذا ظهر الأمن السيبراني ليقوم بدور في حماية الأمن القومي ، وصار اكثر اهتماماً من كافة الفاعلين الدوليين في ظل التطور السريع في وسائل الاتصال وبروز الفضاء الإلكتروني الذي تسير فيه الكثير من الأعمال عن بعد عن طريق الحواسيب الإلكترونية والهواتف الذكية وتطبيقاتها وبرامجها وغيرها من الاجهزة المتصلة بالشبكة الدولية للمعلومات (الإنترنت) . فمع تطور الاجهزة الإلكترونية المرتبطة بالإنترنت واكتشاف برامج وتطبيقات اختراق تلك الاجهزة صار من الضروري على اصحاب تلك الاجهزة خاصة الدول من اخذ احتياطات أمنية لتصدي لمثل هذه الخروقات حفاظاً على ما تحويه هذه الاجهزة من معلومات وبيانات مهمة من السرقة والتدمير والابتزاز والتشفير .

ذكرت المصادر بان بروز مفهوم الأمن السيبراني (CyberSecurity) في عام 1972م ومنذ ذلك التاريخ صار الأمن السيبراني محور اهتمام الدول خاصة الغربية والصناعية (10) .

الأمن السيبراني يتكون من مجموعات من المعلومات والعمليات الرقمية من أجل التوصل الى البيانات والوثائق الرقمية وتأسيس سد إلكتروني يقوم بحمايتها من أي هجمات سيبرانية .

تتم الحماية من الهجمات السيبرانية وذلك بواسطة حماية الاجهزة الإلكترونية المرتبطة بالإنترنت من الاختراق أو التهكير الخارجي والتي تسبب الضرر لكافة جوانب الأمن القومي ؛ لهذا فان الأمن السيبراني له دور في حماية الأمن القومي سيبرانياً . هناك الهاكر وهو عكس الهكر حيث يقوم الهاكر بمحاولات لاختراق الانظمة الإلكترونية والكشف عن أي ثغرات . يعتبر الهكر جزء من الامن السيبراني وهو محلل له يختص بتحليل النظام ومعرفة الثغرات الموجودة في الانظمة من اجل الدفاع عنها وحمايتها من أي خروقات سيبرانية وكذلك إعطاء تقارير لغرض اصلاحها (11) .

بينما هناك هاكر اخلاقي تستعين به مؤسسة ما من اجل اختراق نظام حماية لغرض تحديد الثغرات الأمنية ليضع لها الحلول (12) .

جاء في القانون رقم (5.20) بشأن الأمن السيبراني لدولة المغرب بأنه " مجموعة من التدابير والاجراءات ومفاهيم الأمن وطرق ادارة المخاطر والأعمال والتكوينات وأفضل الممارسات التنكولوجيات التي تسمح لنظام المعلومات أن يقاوم أحداثاً مرتبطة بالفضاء السيبراني ، من شأنها أن تمس بتوافر وسلامة

سرية المعطيات المخزونة او المعالجة او المرسلة ، والخدمات ذات الصلة التي يقدمها هذا النظام أو تسمح بالولوج إليه " (13) .

كما عرف الأمن السيبراني بأنه " عبارة عن علم أو منظومة ظهر مع ظهور الاجهزة الإلكترونية المتطورة مثل اجهزة الكمبيوتر ، الهواتف الذكية وتطبيقاتها ، وغيرها من الاجهزة المرتبطة بالإنترنت "

كما عرف الأمن السيبراني " هو العملية التي تتم من خلالها حماية الاجهزة الإلكترونية المختلفة ، وشبكات الإنترنت ، من أي هجوم سيبراني من الممكن التعرض له " . . . كما قيل بأنه " مصطلح يطلق على كل ما هو له علاقة بالشبكات الإلكترونية عبر الحواسيب ، وشبكات وتطبيقات الإنترنت ، و كل ما له علاقة بالشبكات الاجتماعية مثل : الفيس بوك ، تويتر، رديت ، تمبلر، ويتضمن أيضاً برامج التواصل الفوري مثل واتساب، تيليجرام، الانستقرام وغيره." . . . ، وقيل كذلك هو : " العلم الذي يعمل على حماية شبكات الاتصال والإنترنت والشبكات المهمة في الدول من الاختراق او التجسس ، وذلك عن طريق توفير الحماية القصوى للمعلومات والبيانات التي توجد داخل هذه الشبكات الحساسة والمهمة"(14) .

وطبعاً هذه الحماية تتم عن طريق حماية الأجهزة الإلكترونية من أي اختراقات تضر بجوانب الأمن القومي ولهذا فان الأمن السيبراني يقوم بحماية وتأمين جوانب الأمن القومي في الفضاء السيبراني .

كما عرف الأمن السيبراني بانه " هو ممارسة حماية أجهزة الكمبيوتر والشبكات وتطبيقات البرامج والأنظمة الهامة والبيانات من التهديدات الرقمية المحتملة " (15) .

كما عرف بانه " هو الجهد المستمر لحماية الانظمة والبيانات المتصلة بالشبكة من الاستخدام غير المصرح به " . . . وقيل بانه " عملية حماية الانظمة والشبكات والبرامج ضد الهجمات الرقمية "(16) .

وهناك من يقول :- "هو مجموعة من التدابير والإجراءات التي تتخذها المؤسسات والأفراد لحماية أنظمتهم وبياناتهم الرقمية من الهجمات الإلكترونية والتهديدات السيبرانية "(17) .

وقيل بانه " هو ممارسة الدفاع عن أجهزة الكمبيوتر، والخوادم، والأجهزة المحمولة، والأنظمة الإلكترونية، والشبكات، والبيانات من الهجمات الخبيثة"(18) .

كما عرف الأمن السيبراني بأنه " عبارة عن مجموع الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام الغير مصرح به و سوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني "(19) .

من خلال هذا التعريف يتضح بان الأمن السيبراني يضم مجموعة من الوسائل التي تستخدم كدروع وحصون لحماية الفضاء الإلكتروني من أي خروقات وهجمات سيبرانية من قبل الغير وهي :-

1- إيجاد مجموعة من الوسائل التقنية .

2- وضع مجموعة من الوسائل التنظيمية.

3- وضع مجموعة من الوسائل الإدارية .

وكل هذه الوسائل هدفها منع الخروقات والهجمات السيبرانية ولمنع الاستخدام الغير مصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تضمها .

إذن هنا نجد ان هذا التعريف يوضح لنا بعض الحلول والمعالجات التي تحمي الفضاء الإلكتروني او السيبراني من أي هجمات سيبرانية متوقعة .

إذن نستطيع ان نقول بان الأمن السيبراني هو علم حديث من العلوم الأمنية يهدف إلى حماية كافة جوانب الأمن القومي في الفضاء السيبراني من خلال حماية شبكات الاتصال والإنترنت والأجهزة المتصلة بها من أي هجمات سيبرانية .

إذن نستطيع أن نعرف الأمن السيبراني تعريفاً مختصراً وشاملاً من خلال القول بأن الأمن السيبراني هو وسيلة امنية وعلمية الغرض منها حماية كافة جوانب الأمن القومي سيبرانياً .

بمعنى أن الأمن السيبراني هو الوسيلة الأمنية والعلمية التي تقوم بحماية كافة جوانب الأمن القومي العسكرية والسياسية والاقتصادية والاجتماعية والثقافية والبيئية وما يتفرع من هذه الجوانب من فروع تخص الأمن القومي وتلك الحماية تكون في المجال أو الفضاء السيبراني .

إذن هنا يتضح دور الأمن السيبراني في حماية الأمن القومي وتكون تلك الحماية في الفضاء الإلكتروني أو السيبراني .



ب- أهمية الأمن السيبراني :

1- يعد الأمن السيبراني عنصراً مهماً في تأمين الذكاء الاصطناعي فنظراً لسرعة وقوة وابتكار الهجمات السيبرانية فان الذكاء الاصطناعي في خطر ؛ ولهذا لا جدوى من تواجد الآلات والمعدات التي تسير بالذكاء الاصطناعي في الدول التي لا تهتم بالأمن السيبراني بجدية فأي هجمة سيبرانية قد تؤدي بأضرار في الكثير من جوانب الأمن القومي وفروعه وشعبه المختلفة ، وفي نفس الوقت قد يؤثر الذكاء الاصطناعي في الأمن السيبراني خاصة عندما يستخدم في المساعدة في هجمات سيبرانية على انظمة وشبكات الإلكترونية . إذن هنا تكمن أهمية الأمن السيبراني في تأمين الذكاء الاصطناعي .

2- حماية الانظمة والشبكات والاجهزة الإلكترونية من الهجمات السيبرانية .

3- يعزز إنتاجيات المؤسسات والافراد وذلك من خلال مسح الفيروسات وابراز جدران الحماية والنسخ الاحتياطية ، وكذلك توعية وتثقيف المستخدمين للشبكة الإنترنت بمخاطر التصيد الاحتيالي عبر البريد الإلكتروني والروابط المشبوهة (20) .

4- الأمن السيبراني يهتم بأمن المعلومات الإلكترونية وهذه المهمة يهتم بها أمن المعلومات كذلك . إذن هنا نجد أن هناك علاقة تعاونية بين الأمن السيبراني وأمن المعلومات .

5- يهتم الأمن السيبراني بأمن كل ما هو متوفر في الفضاء الإلكتروني او السيبراني .

6- الأمن السيبراني يقوم بحماية المعلومات والحفاظ عليها .

7- الأمن السيبراني يمنع التطبيق الإلكتروني من التجسس على المستخدم وابتزازه .

8- الأمن السيبراني لكونه نظام إلكتروني يحمي الاجهزة الإلكترونية والتصدي للتجسس على الإنترنت من تلقي الفيروسات ، كما انه يقوم بتنبيه المستخدم باي اخطار ليتخذ التدابير اللازمة لتخلص من تلك الاخطار ، والتي قد تؤدي الى سرقة بياناته او تدميرها .

9- الأمن السيبراني يستطيع ان يتتبع المتسلل الإلكتروني ومعرفة هويته وجمع الكثير من المعلومات عنه مع استطاعت الأمن السيبراني ان يقدم كافة التهم للمتسلل معترف به قانوناً .

10- الأمن السيبراني يساهم في الوصول الى كافة البيانات وجميع الهوايات التي تصل الى بيانات المستخدم بشكل قانوني او غير قانوني .

11- الأمن السيبراني بالإمكان ان يحدد موقع المستخدم ونشاطه وتفاعله مع البيئة الخارجية وذلك من خلال الاتصال بعدد من المنصات الرقمية بواسطة برنامج إلكتروني يستخدمه المستخدم .

12- يعمل على حماية بيانات مستخدم التطبيق وشبكات الإنترنت في حال كان المستخدم له خلفية ثقافية في الاستخدام الصحيح للأمنين السيبراني والمعلومات .

ج- اهداف الأمن السيبراني :

اشارت الدراسات البحثية بخصوص الأمن السيبراني بان اهدافه كثيرة منها حماية الأنظمة والشبكات والبرامج من الهجمات الإلكترونية او الرقمية من مخترقين هدفهم حذف أو تشفير بيانات او استيلاء على معلومات او تدمير بيانات او من اجل الابتزاز عبر الفضاء السيبراني .إذن هناك اهداف كثيرة للأمن السيبراني من أهمها الاتي :-

1-حماية الانظمة الإلكترونية المربوطة على الشبكة الدولية للمعلومات (الإنترنت) من الهجمات السيبرانية التي يقوم بها المخترقون .

2-حماية الشبكات الإلكترونية من الهجمات السيبرانية.

3-حماية البرامج والمتواجدة على الحواسيب الإلكترونية والهواتف الذكية المربوطة على (الإنترنت) من الهجمات السيبرانية (21).

حيث تلجأ المؤسسات والافراد الى وضع احتياطات الأمان من اجل تأمين حواسيبهم المرتبطة بالإنترنت ، والتي تكون عرضة للهجمات السيبرانية والمتواجد بها بياناتهم وملفاتهم الشخصية ومعلوماتهم الحساسة وكل ما يتعلق بحياتهم الشخصية والوظيفية .

4-تطبيق التقنيات والاجراءات والضوابط التي تهدف الى الكشف عن اي خروقات وتهديدات.

5-الوقاية من الهجمات السيبرانية .

6-القدرة على استعادة واسترداد البيانات التي قد تتعرض للخروقات (22) .

7-حماية شبكات الاتصال والإنترنت والشبكات المهمة في الدولة من الاختراق من خلال توفير حماية سيبرانية للمعلومات والبيانات التي تحويها تلك الشبكات والاجهزة من بيانات وتطبيقات وبرامج .

د- أنواع الأمن السيبراني :

وفق ما جاء في الكثير من الدراسات فان انواع الأمن السيبراني كثيرة اهمها الاتي :-

1-**أمن الشبكات** : وقد اشير بان هذا النوع يختص بالحماية والمحافظة البنية التحتية للشبكات والبيانات التي تسبح فيها من الهجمات السيبرانية ، وذلك بواسطة عدة وسائل دفاعية كجدار الحماية والذي يستخدم من اجل منع الوصول غير المصرح به ، وكذلك استخدام نظام كشف التسلل السيبراني من اجل رصد الانشطة المشبوهة والتنبيه من خطرها ، وكذلك أمن فبن (Vpn) وذلك من اجل تأمين الاتصالات عبر الشبكة الدولية للمعلومات الإنترنت(23) .

2-**أمن البيانات :** يقوم هذا الأمن من انواع الأمن السيبراني بالتركيز على حماية البيانات من التسريب والتلف او الاستخدام غير المصرح به ، تتم هذه الحماية بعدة وسائل مثل التشفير والذي هو عملية تحويل البيانات الإلكترونية إلى رموز غير معروفة ومفهومة من الصعب قراءتها او معرفتها دون إعادتها إلى سابق ما كانت عليه ، والغرض من هذا الأمن هو حماية البيانات اثناء النقل والتخزين ، وكذلك بواسطة إدارة البيانات ، والتي تهدف الى ضمان ان البيانات تستخدم وتخزن بشكل أمن ، وايضاً تتم الحماية بواسطة النسخ الاحتياطي والغرض من ذلك هو استعادة واسترداد البيانات في حال حذفها او اتلافها .

3-**أمن النهايات :** الغرض من هذا الأمن هو حماية الاجهزة المتصلة بالشبكة كالحواسيب والهواتف الذكية وهذا النوع يستخدم الحماية عن طريق عدة وسائل كبرنامج مكافحة الفيروسات والذي يهدف لمسح ومنع البرمجيات الخبيثة ، وكذلك استخدام إدارة التحديثات من اجل التأكد من ان كافة الاجهزة تستعمل أحدث البرامج والإصلاحات الامنية ، وكذلك بواسطة التحكم في الوصول من اجل ضمان ان المستخدمين المصرح لهم فقط بأمكانهم الوصول الى الاجهزة والبيانات . هذا وقد اشير بان هذه الانواع من الأمن السيبراني تؤمن الأمن السيبراني كاملاً(24) .

4-**أمن التطبيقات** : وهذا النوع من الأمن السيبراني يستخدم مع مراحل تطوير البرامج وبعد نشرها ، ويتم ذلك بواسطة اختبارات الاختراق والتي بواسطتها يتم تحديد الثغرات الأمنية في التطبيقات ، وكذلك بواسطة تحديثات الأمان لغرض اصلاح الثغرات والحفاظ على أمن التطبيقات ، وكذلك بواسطة الحماية من البرمجيات الخبيثة من اجل منع تثبيت البرمجيات الضارة (25) .

إذن هناك عدة أنواع للأمن السيبراني وهي أمن البيانات وأمن الشبكات وأمن التطبيقات وامن النهايات والجنود الذين يستخدمون الوسائل الدفاعية والهجومية هم الفئة الفنية المتخصصين في تقنية

المعلومات والحاسوب والاتصالات والتكنولوجيا وسياساتها تضع من متخصصين في الأمن القومي بناءاً

على تقارير واستشارات الفئة الفنية .

ر- علاقة الأمن السيبراني بالأمن القومي :

1-الأمن والأمن القومي المفهوم والجوانب :

نتيجة تشابك المجتمعات البشرية وعيشها في تجمعات وشعورها بالأخطار التي تهدد وجودها صارت تفكر بما يحفظ أمنها الاقتصادي والاجتماعي والسياسي والبيئي والثقافي ، فكان العسكري أولاً وكان البيئي اخيراً . بدأت المجتمعات البشرية في تنظم نفسها وتضع نظم لمراقبة سير حركات الأفراد مع توجيههم وإرشادهم وإعدادهم لمواجهة أي أخطار خارجية قد تأتي من الخارج ، وتطورت هذه المهمة وصارت تنتقل من الفرد إلي الجماعة ثم إلي القبيلة ، وصارت تنظم صفوفها لمواجهة أي عدوان خارجي ، وهذا من أجل حماية الفرد والجماعة وتأمين حياتهم ومع مرور السنوات صارت الدولة هي المسؤولة عن توفير الأمن لمواطنيها داخلياً وخارجياً . أستمر مفهوم الأمن وكما يشير المتخصصون لا يتعدى مواجهة الأخطار التي تهدد الدولة خاصة الغزو العسكري إلي أن ظهرت " الدولة القومية " بعد صراع مرير على السلطة والحكم والتحكم فصار نشاط الدولة يتسع فشمل جوانب متعددة حيث شمل البيئة الداخلية والبيئة الخارجية ، وبظهور الدولة القومية ظهرت مفاهيم جديدة للأمن كان من ضمنها الأمن القومي لضمان أمن الدولة القومية ، وصار هذا المفهوم يتطور بسرعة خاصة في أوروبا التي نشأ فيها بداية ما يسمى بالدولة القومية بعد صراع مرير مع المؤامرات والحروب وقد اتضحت معالمه وحدوده في الولايات

المتحدة الأمريكية وأوروبا بينما لازال في حالة غموض في الدول النامية والتي من ضمنها ليبيا . ونفس الشعور السابق الذي شعرت به التجمعات البشرية تجاه الأخطار التي تهدد أمنهم السيبراني لهذا فكرت في استحداث الأمن السيبراني وهو في حد ذاته يعتبر وسيلة أمنية علمية لحماية الأمن قومي ؛ لأنه يحمي كافة جوانب الأمن القومي سيبرانياً .

يقصد بالأمن في هذه الدراسة ليس الأمن في مضمونه الضيق داخل حدود الجانب العسكري والذي يعتبر أمن نسبي ، بل يقصد به الأمن الذي يشمل كافة جوانب الأمن ألا وهو الأمن القومي أو الوطني للدولة ، هذا الأمن الذي يحتوي على كافة جوانب الحياة التي تهم الانسان وحتى الحيوان والطير والنبات فالأمن البيئي مثلاً يهم الانسان والحيوان والنبات . المقصود به هو الأمن المطلق نسبياً حيث لا يوجد أمن مطلق حتى في الدول العظمى انما هو نسبي يتفوق على الكثير من دول العالم في توفير الكثير من جوانب الأمن .

الأمن هنا نقصد به الأمن القومي او الوطني كما يحب البعض ان يطلق عليه ، هذا الأمن الذي يحوي كل الجوانب التي عند تأمينها تجلي الخوف من الذين يحتويهم هذا الأمن بل انه يقوم بحماية حتى الجماد الذي يحيطهم فالذين يشعرون بالخوف قد يكونوا من البشر او الحيوان او الطير او حتى النبات فكل منهم يشعر بالخوف بطريقته كالشعور بتوقعاته لما هو اتي من عوامل تؤثر على حياته ، والخوف هذا وقتي ينتاب من يحط به والذي يقوم بوضع تدابير وسياسات عامة ليتجنب اخطار وصدامات هذا الخوف .

بدأ الاستخدام بمصطلح الأمن الوطني او القومي مع نهاية الحرب العالمية الثانية وتحديداً عام 1947م حيث قامت الولايات المتحدة حينها بتأسيس مؤسسة تخص الأمن الوطني او القومي وهي (مجلس الأمن الوطني الامريكي) وقد اسندت اليه كافة الامور والاحداث التي تمس كيان الدولة الامريكية وتهدد كيانها . بعد الحرب الباردة تغير مفهوم الأمن الذي كان ينعى في مضمونه الجانب العسكري الى جوانب اخرى تهم العالم باسره .

ويؤكد الباحث والخبير الأمني (والت) ذلك بالقول :- " ان القوة العسكرية مهمة ولكن لا يمكن لها ان تكون الضامن الوحيد للأمن الوطني ، فالتهديدات العسكرية لا تمثل أبداً التهديدات الوحيدة في البيئة الجديدة" .

كما أكد ذلك (لورنس فريدمان) بالقول :- " ان أي شيء يبعث القلق ويهدد نوع الحياة يوسم بانه مشكلة امنية . . فالدفاع عن الامة ضد داء معدٍ مشكلة تختلف تماماً عن مواجهتها لهجوم بالصواريخ الباليستية "(26) .

واشير بان الأمن لا يأتي بالمعدات العسكرية وحسب وان كان يتضمنها ، وهو كذلك ليس موجهاً ضد التهديدات الخارجية وحسب ، انما يشمل أيضا التهديدات الداخلية(27) .

عرف الأمن القومي عدة تعريفات للكثير من الأساتذة وعلماء السياسة والأمن لعدم اتفاق على تعريف معين وكذلك لتطور المفهوم فبعد أن كان لا يتخطى الجانب العسكري صار يضم جوانب أخرى منها الاقتصادي والسياسي والاجتماعي والثقافي والبيئي وغيرها . أعطاه أمين هويدي في كتابه (الأمن العربي في مواجهة الأمن الإسرائيلي) تعريفاً يقول : " عبارة عن الإجراءات التي تتخذها الدولة في حدود طاقاتها للحفاظ على كيانها ومصالحها في الحاضر والمستقبل مع مراعات المتغيرات الدولية " (28) .

بالنظر لهذا التعريف نجد انه يحاكي الأمن السيبراني في الإجراءات التي تتخذها الدولة للحفاظ على كيانها ومصالحها حاضراً ومستقبلاً ، وطبعاً الاجراء المتخذة تكون في كافة الجوانب التي تحافظ على كيان الدولة ومن فيها كتوفير الأمن الاقتصادي السيبراني والأمن السياسي السيبراني والأمن الاجتماعي السيبراني والأمن البيئي السيبراني والأمن الثقافي السيبراني ؛ ولهذا نجد دول واعية تأخذ خططها واستراتيجياتها وسياساتها العامة من جهاز امنها القومي ، وهذا غير موجود في ليبيا رغم ان قانون رقم (4) لسنة 2007 الخاص بإنشاء مجلس الأمن الوطني اعطاءه اختصاصات واسعة تمكنه من وضع كافة سياسات المؤسسات الحكومية بما فيها الجيش والشرطة وما يتبعهما من اجهزة أمنية(29) .

من خلال ذلك نجد ان هناك علاقة بين الأمن القومي والأمن السيبراني فالأمن السيبراني هو أمن قومي سيبراني يحوي كافة جوانب الأمن القومي التقليدي كالجانب الاقتصادي والسياسي والعسكري والانساني

والبيئي والاجتماعي . إذن هنا نستطيع أن نقول بان الأمن السيبراني هو وسيلة أمنية لحماية الأمن القومي خاصة الذي قد يتعرض لتهديدات سيبرانية إذن نستطيع ان نقول بان هناك علاقة وثيقة بين الأمن السيبراني والأمن القومي .

كما أعطاه (محمد عبدالكريم نافع) في كتابه (الأمن القومي ،ج1) تعريفاً يقول بأنه :- " ما تتخذه الدولة من إجراءات في مختلف المجالات ،على أنه الجهد اليومي الذي يصدر عن الدولة لتنمية ودعم أنشطتها الرئيسية السياسية والاقتصادية والاجتماعية والعسكرية ، ومنع ما يسبب عرقلة هذه الأنشطة"(30) .

وهنا نجد أن يتضح لنا بان الأمن السيبراني وسيلة من الوسائل حماية الأمن القومي سيبرانياً .

كما أعطاه (علاء طاهر) تعريفاً يقول بأنه " مجموعة من التدابير والاحتياطات النظرية والعملية الخاصة بحماية المجال الإقليمي لدولة ما، وثرواتها ، وأيديولوجيتها وسياستها الخاصة بما فيها الأهداف الوطنية الممثلة لخصوصيتها القومية والحضرية " (31) .

وعرفه (دومنيك دافيد) بالقول :- " الأمن في معناه الواسع يتمثل في الخلو من التهديدات او أي شكل للخطر وتوفر الوسائل اللازمة للتصدي لذلك للخطر في حال اصبح أمراً واقعاً "(32) .

كما عرف البعض بان المقصود بالأمن هو " حالة الثقة والهدوء عند من يعتقد نفسه في مأمن من كل خطر، كما أنه يعني تنظيم شروط مادية اقتصادية وسياسية كفيلة بخلق هذه الوضعية ، وهو يصف الإجراءات والأشياء الكفيلة بضمان أمن المعنيين"(33) .

من التعريف السابق يتضح لنا بان الأمن القومي هو حالة من الاستقرار وتأمين من الأخطار إضافة إلى انه تنظيم اقتصادي وسياسي إذن الأمن هنا وسيلة هامة للمحافظة على الهدوء والاستقرار والحماية من أي اخطار ، وهو كذلك تنظيم القصد منه حماية المواطنين وكافة الأحياء التي معهم والمحافظة الجماد والبيئة التي يعيشون فيها من أي اخطار تهددهم ، وفي المقابل نجد ان الامن السيبراني يحافظ على أمن الدولة سيبرانياً وهو بهذا له علاقة بالأمن القومي لكونه هو الآخر أمن قومي ولكن اجراءاته سيبرانية ، وبهذا فان الأمن السيبراني هو وسيلة لحماية للأمن القومي سيبرانياً .

عرفته دائرة المعارف البريطانية بأنه " يعني حماية الأمة من خطر القهر على يد قوة أجنبية " . . . كما عرفته دائرة معارف العلوم الاجتماعية بأنه " يعني قدرة الدولة على حماية قيمها الداخلية من التهديدات الخارجية " ، كما عرفه (هنري كيسنجر) بأنه " أي تصرفات يسعى المجتمع عن طريقها إلى حفظ حقه في البقاء " ، أما روبرت كما نجد من يعرفه بأنه " هو التنمية ، وبدون تنمية لا يمكن أن يوجد أمن ، وأن الدولة التي لا تنمو بالفعل ، لا يمكن ببساطة أن تظل أمنة " (34) .

نجد ان تعريف دائرة المعارف البريطانية يشكل فيه الأمن العسكري جانب كبير رغم ان القهر قد يأتي من الجانب الاقتصادي والسياسي والاجتماعي ، وهذا مرت به الصين ابان الاحتلال الانجليزي الذي نشر الافيون وهدد الأمن الاجتماعي فيها والاقتصادي والسياسي ، وهذا ما تمر به ليبيا الأن خاصة في الجانب السياسي والاقتصادي والبيئي والاجتماعي والثقافي ، كما ان تعريف دائرة معارف العلوم الاجتماعية نجده يشير الى ان الأمن القومي وهو الأمن الشامل يتطلب حماية من التهديدات الخارجية وهذه التهديدات قد تكون اقتصادية تحتاج الى أمن اقتصادي او اجتماعية تحتاج الى أمن اجتماعي او ثقافية تحتاج الى أمن ثقافي او بيئية تحتاج الى أمن بيئي ، أما في تعريف كيسنجر نجد ان لتحقيق الأمن الوطني او القومي هو ان تسعى الى تدابير للحفاظ على البقاء وطبعاً هذا يتطلب تدابير لتأمين كافة جوانب الأمن القومي ، أما في تعريف ماكنمارا نجد ان لتحقيق الأمن القومي او الشامل هو بإحداث تنمية ونجاح وتحقيق أهداف هذه التنمية.

هناك من يقول بأن الأمن القومي هو حماية الوطن والشعب من أي اعتداء أو عدوان خارجي عن طريق عدة وسائل تعكس المصالح السياسية والاقتصادية والحيوية للدولة وبالتالي فأن تهديد أو فقدان الدولة لأي من مصالحها العسكرية أو الاقتصادية فيه تهديد مباشر أو غير مباشر لوجود الدولة (35) .

كما ركز محمد فوزي في كتابه (حرب الثلاث سنوات) على عوامل الخطر في تحديده والذي يتمثل في سلامة وأمن المجتمع ويتحقق بإدراك الظروف السياسية والاقتصادية والاستراتيجية ، وهو يتفق بأن الأمن القومي ليس عسكرياً فقط وبهذا فأنه يتفق مع النظرية الشمولية التي تستجوب توفر عوامل كثيرة مثل السياسة والاقتصاد والقوة العسكرية . .الخ (36) .

كما عرف الأمن القومي بانه " طمأنينة بالنسبة لكل ما يتصل بالتعبير عن الوجود السياسي والالتزام بالولاء والطاعة ازاء السلطة ، اما الطمأنينة فهي تعني : الاستقرار والقدرة على مواجهة المفاجآت المتوقعة وغير المتوقعة ، دون ان يترتب على ذلك اضطراب الاوضاع بما يقلص الطمأنينة والاستقرار " (37) .

كما نجد (روبرت ماكنمارا) " في كتابه " جوهر الأمن" يعرف الأمن القومي بانه " يعني الأمن التطور والتنمية سواء الاقتصادية منها او الاجتماعية او السياسية ، في ظل حماية مضمونة "(38) .

كما اشير بان (ماكنمارا) قال في الامن القومي كذلك : "الأمن الحقيقي للدولة ينبع من شعورها العميق للمصادر التي تهدد قدرتها ومواجهتها لإعطاء فرصة لتنمية تلك القدرات تنمية حقيقية في كافة المجالات سواء في الحاضر او المستقبل"(39) .

كما عرف الأمن القومي من قبل (توماس شيلينج) بانه :- "الكيان الذي يسعى الى الحفاظ على الدولة حرة ، مع ضمان فاعلية القيم والمؤسسات الرئيسية بها "... كما عرفه (اورنولد وونفرز) أنه :- " غياب أي تهديد للقيم المركزية للدولة"(40) .

إذن من خلال ما تقدم من تعريفات للأمن القومي نجد أن هناك علاقة بين الأمن السيبراني والأمن القومي حيث يتضح بان الأمن السيبراني هو احد الوسائل التي تحمي الأمن القومي خاصة في الفضاء السيبراني .

2–جوانب الأمن القومي :

قسم بعض من المتخصصين في الأمن وعلماء السياسة الأمن إلي الاتي :–

2/1– الأمن السياسي . 2/2– الأمن الاقتصادي . 2/3– الأمن الاجتماعي .

2/4– الامن العسكري . 2/5– الأمن الأيديولوجي . 2/6– الأمن البيئي .

2/1– الأمن السياسي : وهو يهدف للمحافظة على حرية الإرادة الوطنية وحرية اتخاذ القرار وتأمين السياسة الوطنية والقومية والمستقبلية للدولة . وقد عرف بأنه " الجهود المبذولة في المحافظة على أسرار الدولة وسلامتها ، والعمل على منع ما من شأنه إفساد العلاقة بين السلطة والشعب أو تشويه صورة الدولة "(41) .

هذا الجانب ذو شقين الاول يتمثل في السياسة الداخلية هو لإدارة المجتمع ومحاولة التغلب على ما يتعرض له من مشاكل ، والسعي نحو تحقيق تماسك الدولة ، والتوافق بين افراد الشعب الواحد وما يسير الدولة ، وهذا الشق يرتبط بعدة مرجعيات امنية هي الدول ، والمنظمات الدولية ، والحركات العابرة للحدود الوطنية ، اما الشق الثاني يتمثل في السياسة الخارجية وهي تهدف لتحقيق مصالح الدولة من خلال تأثيرها على المجتمع الدولي (42) .

وهذا الجانب يكاد يكون معدوم في الكثير من الدول مثل ليبيا فأسرار الدولة والكثير من ملفاتها السرية عند دول اجنبية. وهذا الجانب تمرر الكثير من بياناته ومعلوماته على الإنترنت ويتعرض للهجمات السيبرانية وهو يحتاج الى أمن سيبراني .

2/2- الأمن الاقتصادي : يهدف هذا الجانب إلى تأمين اقتصاد الدولة ضد أي تهديدات سواء كانت داخلية أو خارجية والمحافظة على التوازنات الاقتصادية المختلفة وتحقيق قدر من الاكتفاء الذاتي والرخاء والعدل للدولة . وهذا الجانب معدوم في الكثير من الدول مثل ليبيا . وهذا الجانب هو الآخر بياناته ومعلوماته تواجدت على الاجهزة الإلكترونية مربوطة على الشبكة الدولية للمعلومات . وهو مهدد بالهجمات السيبرانية ويحتاج لأمن سيبراني .

2/3- الأمن الاجتماعي : ويهدف هذا الجانب للمحافظة على المجتمع من أي صراعات طائفية أو قبلية أو عنصرية ، وكذلك يهدف للمحافظة على المجتمع من تفشي الجريمة وانتشار الامراض الاجتماعية الأخرى ، ويطلق على الأمن الاجتماعي أسماء متعددة منها التماسك الاجتماعي والقوة الاجتماعية ، ويقصد به كما ذكر المتخصصون الحالة التي يكون فيها المجتمع متماسكاً (43) .

وهذا الجانب كذلك غير متوفر في الكثير من الدول مثل ليبيا وان كان هناك من يعتقد بانه متوفر .

2/4- **الامن العسكري** : والهدف منه كما يشير المتخصصون هو حماية الدولة ضد أي تهديدات خارجية مع تحقيق الاستقرار الداخلي في إطار الشرعية وأن يكون ولاء الجيش للغايات والأهداف الوطنية او القومية للدولة بعيداً عن الطائفية والقبلية والحزبية . وهذا الجانب توفرت بياناته ومعلوماته وتطبيقاته وأعماله في الفضاء السيبراني مما يعرضه للتهديد من قبل الهجمات السيبرانية من دول ومنظمات وحتى افراد خاصة في غياب الأمن السيبراني .

2/5- **الأمن الثقافي** : والغاية منه هو تأمين الدولة وشعبها ضد أي غزو ثقافي أجنبي مضر بأفكار الدولة والقضاء على أي أفكار هدامة وافدة من الخارج . ويعتبر المحافظة عليه من اصعب الامور بسبب التطور الذي حدث في ثورة المعلومات والاتصالات التي صارت تفرض على أي دولة تحديات صعبة بسبب الخروقات التي لا تستطيع أي دولة ان تمنعها بعد ان تطورت وسائل اتصال المعلومات التي صارت تدخل كل بيت دون عناء وتعب(44) .

وهذا الجانب هو الآخر يتطلب تدخل أمني سيبراني من الدولة لحمايته من أي اعتداءات سواء على بياناته وتطبيقاته وملفاته المربوطة على الشبكة الدولية للمعلومات ، إضافة الى البرامج التي تهدف الى طمس الجانب الثقافي في الدولة ، فالهجمات السيبرانية على هذا الجانب باستمرار بسبب البرامج التي تبث وتعرض عبر شبكات التواصل المختلفة وحتى تلك التي تبثها وتعرضها القنوات الفضائية .

2/6– الأمن البيئي :يهدف إلى حماية الدولة من أخطار التلوث البيئي كتلوث الأجواء والبحار والمحيطات والأنهار والأرض والغذاء وكل ما يخص الدولة ، وهذا الأمن يعتبر أمناً إقليمياً ودولياً ؛لأن البيئة تخص كل سكان الكرة الارضية ، وقد بدأ هذا المفهوم أكثر انتشاراً وفق ما ذكره العديد من المتخصصين في السبعينات من القرن العشرين ، وصار يتداول من قبل المنظمات الدولية وخاصة في الأمم المتحدة حيث بدأت المخاطرة تتضح بقوة نتيجة لتلوث البيئة أرضاً ومياه وهواء نتيجة المخلفات الضارة حتى وصلت إلى تهديد الوجود البشري برمته نتيجة لتصاعد السموم والغازات إلى طبقات الهواء العليا وغلاف الكرة الأرضية(45) .

وتأكيداً على شمولية الأمن القومي للأمن البيئي ما اكده العالم والباحث ماثيوس الذي قال :– " التطورات العلمية الحالية تشير الى تعريف اكثر اتساعاً للأمن الوطني بإدراج المسائل الخاصة بالمصادر البيئة والسكان "(46) .

وعلى شمولية الأمن القومي كذلك أكدت دراسة على الأمن الوطني الاردني حيث نجدها تقول في احد مرتكزات الأمن :– " الامن الاقتصادي والاجتماعي للشعب الاردني بفئاته المختلفة ركن اساسي من اركان امنة الوطني يستلزم زيادة قدرة الوطن في الاعتماد على الموارد الذاتية ، وتمكينه من تلبية الحاجات الاساسية للشعب . بما يحفظ كرامة المواطن ، ويسهم في توفير امنه المادي والمعيشي والنفسي "(47) .

كما تأكد دراسة أخرى على شمولية الأمن بالقول :- " ان الأمن بمفهومه الشامل لا يقتصر على جانب دون سواه وعندما نقول الأمن الوطني الشامل يعني ذلك الأمن السياسي ، والاقتصادي ، والاجتماعي ،والعسكري ،والتقني ،والمعلوماتي ، وكل شيء يهم الافراد والاسر والمجتمعات والدول والعالم اجمع على حد سواء"(48) .

اذن الأمن السيبراني يشمل تأمين كافة جوانب الأمن القومي وهو وسيلة لها دور في حماية الأمن القومي خاصة سيبرانياً فحماية الفضاء السيبراني للأفراد والمؤسسات عامة وخاصة من أي خطر او تهديد لأجهزتهم وتطبيقاتهم وبياناتهم وبرمجياتهم وشبكاتهم المربوطة على الإنترنت التي قد تتعرض لها بواسطة الاختراق او التشفير او التدمير او الابتزاز هو حماية للأمن القومي بمعنى ان يتم الحماية لكافة الجوانب التي تجعل الافراد في أمان ، كما ان الحفاظ على الدولة حرة وضمان فاعلية القيم والمؤسسات بها يتطلب توفير الأمن الشامل الذي يأمن كافة جوانب الأمن القومي . حقيقة الأمن الآن صار أمناً شاملاً ولتحقيق الأمن لدولة ما صار يتطلب من الدولة توفير الأمن الشامل ، والذي يوفر كافة جوانب الحياة للدولة وسكانها وبهذا فان الأمن هنا أمن مطلق نوعاً ما رغم ان الأمن المطلق لم تحققه أي دولة إلى الآن ،فالأمن الحقيقي ليس هو الأمن المتعارف عليه الآن الذي يركز على الأمن العسكري والسياسي والذي يعد أمناً نسبياً ليس فيه حماية كافية للدولة وسكانها فالأمن العسكري الآن صار يوفر عبر شركات اجنبية خاصة وقد

برهنت حرب افغانستان والحرب الاوكرانية الروسية حيث دافعت (بلاك ووتر) عن أمن أمريكا العسكري ، ودافعت (فاغنر) لصالح الأمن العسكري الروسي ، وعلى هذا المنوال يوجد الكثير . فغياب الأمن الاقتصادي والاجتماعي والبيئي والثقافي يعني ان هناك فوضي في جوانب هذا الأمن وبالتالي لا يوجد تأمين لجوانب الأمن القومي حتى وان شعر المسؤولين بان خطتهم في حماية الأمن القومي تسير على ما هو عليه إلا ان هذا غير صحيح ؛ لان هذا الأمان مؤقت وعلى صفيح ساخن ، وهذا مرت به الكثير من الدول خاصة في الدول النامية ، وخير دليل أين الأمن في ليبيا والذي كان مركز على الجانب العسكري وكانت نفقاته كبيرة ؟ واين الأمن في العراق ، وسوريا واليمن والسودان وغيرها ؟. معظم الدول النامية تعتقد بان أمنها القومي بأمان وهي تركز على الأمن العسكري دون التركيز على الجوانب الاخرى للأمن ، الأمان في هذه الدول على صفيح ساخن ومسألة انفجار الفوضى هي مسألة وقت ، وهذا الانفجار ستكون فيه ردت فعل قوية قد تنهي كيان دول وتقسمها ، وقد تلغي حتى ايديولوجيات ومعتقدات خاصة في غياب الأمن الثقافي .

الأمن السيبراني هو احد الوسائل الأمنية العلمية وهو من ضمن تكوينات الأمن القومي الجديدة بعد التطور في وسائل الاتصال وانتشار الإنترنت على نطاق واسع وصار هذا النطاق والذي يشمل شبكات الإنترنت والفضاء الإلكتروني في حاجة الى أمن يحافظ عليه ويحميه من التهديدات التي يتعرض إليها ، من

خلال هذا نجد ان هناك دور للأمن السيبراني في تأمين جوانب الامن القومي سيبرانياً ، تقول دراسة في الأمن السيبراني :- " لقد بات الأمن السيبراني يشكل جزءاً أساسياً من أي سياسة أمنية وطنية"(49) .

إذن هنا نجد ان الأمن السيبراني جزء من الأمن القومي وهو يختص بحماية الأمن القومي في الفضاء الإلكتروني وهو يحمي كافة جوانب الأمن القومي وفروعها سيبرانياً .

من خلال فروع وجوانب الأمن القومي نجد ان الكثير منها يتواجد داخل الفضاء السيبراني او الإلكتروني فأجهزة الكمبيوتر والشبكات وتطبيقات البرامج والأنظمة الهامة والبيانات والمعلومات لكافة المؤسسات سواء كانت عسكرية او اقتصادية او سياسية او اجتماعية او ثقافية او بيئية تتعرض من حين إلى آخر إلى تهديدات رقمية أو سيبرانية ، وهذا يتطلب توفير أمن سيبراني ليكون له دور في حماية الأمن القومي سيبرانياً . فحماية شبكات واجهزة الدولة الإلكترونية التي تعنى بالاقتصاد من أي خروقات وهجمات سيبرانية فيه حماية للأمن الاقتصادي الذي هو جزء من الأمن القومي ومن هنا نستطيع ان نقول بان هناك أمن اقتصادي سيبراني ، وأمن عسكري سيبراني ، وأمن سياسي سيبراني ، وأمن ثقافي سيبراني ، وأمن اجتماعي سيبراني ، وأمن بيئي سيبراني ، والتي يتطلب من الدول أن توفرها لحماية بيانات ومعلومات وتطبيقات وبرامج جوانب أمنها القومي المربوطة على الشبكة الدولية للمعلومات الإنترنت

. في المجال الاقتصادي عادة ما تقوم بعض الشركات والمؤسسات باحباط منافسيها من اجل التفوق على مؤسسات وشركات اخرى ترتبط اجهزتها وبراجها وبياناتها وتطبيقاتها وشبكاتها على الإنترنت . وهذا يحتاج الى حماية أمنية ، والحماية هنا ستكون ضمن ما يمكننا ان نطلق عليه الأمن السيبراني الاقتصادي . إذن نستطيع ان نقول بان الأمن السيبراني الاقتصادي هو الوسيلة الأمنية والعملية التي يتم فيها حماية شبكات وتطبيقات وبيانات وبرمجيات واجهزة الدولة الإكترونية التي تعنى بالاقتصاد من أي اخترقات وهجمات سيبرانية .

كما يتعرض الأمن القومي في جانبه الاجتماعية إلى هجمات سيبرانية متنوعة مثل بث الثقافات الهدامة من خلال نشر الافلام غير الجيدة والدعاية المغرضة التي تبث افكاراً هدفها تدمير الفكر والاخلاق والآداب العامة للمجتمع خاصة في العادات والتقاليد والمعتقدات الدينية ، ومن تلك الهجمات السيبرانية التي لها تأثير على الأمن الاجتماعي مثلاً هو نشر المخدرات الرقمية التي توازي المخدرات التقليدية حيث يقول أحد المصادر في هذا الصدد :- المخدرات بصفة عامة آفة اجتماعية ابتليت بها جميع الشعوب العربية على غرار باقي الشعوب الأخرى منذ القدم ، وتطورت بتطور الوسائل التقنية الحديثة أو الرقمية تبعث على شكل موسيقى بالنسبة للمدمن تعمل على تدميره نفسياً ، جسدياً ، عصبياً ، كما تدمر

الدول اقتصادياً واجتماعياً ، الامر الذي يمثل تهديداً خطيراً للمجتمعات العربية على وجه الخصوص في ظل عجز المجتمع الدولي عن إيجاد تشريعات دولية للحد من هذه الظاهرة " (50) .

هنا نجد ان الهجمات السيبرانية التي تحدث موجهة الى افراد المجتمع خاصة فئة الشباب الذين يتصفحون مواقع التواصل الاجتماعي المختلفة عبر الشبكة الدولية للمعلومات الإنترنت والسلاح الذي اطلق من تلك الهجمات عبارة عن موسيقى مدمرة للأعصاب والجسد والنفس تجعل المتلقي لها في حالة من الياس والخمول وهذا النوع من السلاح يطلقون عليه حديثاً في العالم السيبراني المخدرات الرقمية فالمخدرات لم تعد مادة نباتية في ظل التطور السريع في التكنولوجيا بل اصحبت إلكترونية ، وطبعاً هذه الهجمات تهدد الامن القومي في جانبه الاجتماعي وحتى الاقتصادي لما ينفق من اموال على قيمة التصفح . هذا النوع من المخاطر تم اكتشافه من قبل الباحثة النفسانية الامريكية كمبرلي يونغ عام 1994م وكان تحت مسمى الأمان السيبراني (51) .

وقد اشير بانه لم يعد تعاطى المخدرات بالطرق التقليدية كالتدخين والحقن والشم والمضغ بل تطور التعاطي بتطور وسائل التكنولوجيا وصارت إلكترونية (52) .

وهذا النوع يتم استقباله عن طريق الحواسيب والهواتف الذكية المربوطة على الإنترنت وهي سهلة التداول وقليلة السعر وسهل الحصول عليها . بتطور وسائل الاتصال توسعت الى المخدرات الإلكترونية. تلك

المخدرات تزود السماعات بأصوات تشبه الذبذبات بقوة اقل من 1000 الى 1500 هيريز ، وهي تروج عبر الإنترنت بشكل MP3 وهناك ترددات لكل نوع من المخدرات (53) .

كما عرفت بانها " نوع خاص من الموسيقى ذات الترددات المميزة والتي يعتقد ان لها تأثير على درجة نشاط المخ واستقباله للألم والتحكم في الحالة النفسية للمستمع " (54) .

ولخطر الهجمات السيبرانية مثل نشر المخدرات الرقمية أو الإلكترونية على الأمن الاجتماعي والثقافي اوصت دراسات باستحداث مواقع وطنية حول الأمن السيبراني تهدف إلى لمساعدة افراد المجتمع لأخذ الحيطة والحذر عند دخولهم الفضاء السيبراني وان يتعرفوا على الخيارات المتوفرة لتأمين نفاذهم للفضاء السيبراني(55) .

من السياسات الأمنية السيبرانية التي استخدمت لحماية الأمن الاجتماعي هو حماية الأطفال المتصفحين لشبكات التواصل عبر الإنترنت حيث قامت الكثير من الدول بوضع ضوابط وتدابير من اجل استحدثت مواقع إلكترونية حول الأمن السيبراني الهدف منه هو مساعدة مواطني الدولة ليتصرفوا بمسئولية في الفضاء السيبراني وتقديم توجهات وارشادات مفيدة لمواجهة الهجمات السيبرانية **(56)** .

هنا نجد ان هناك علاقة بين الأمن السيبراني والأمن القومي في جانبه الاجتماعي إضافة الى ان الأمن السيبراني يعتبر وسيلة أمنية علمية لحماية الأمن القومي .

حماية الأمن الثقافي السيبراني تقع على عاتق الأمن السيبراني فهو له دور في حماية هذا الجانب من جوانب الأمن القومي . هذا الجانب حقيقة غير متوفرة في الكثير من الدول من بينها ليبيا والدليل على ذلك اعتناق بعض الشباب المسيحية مما هدد الأمن الثقافي او الفكري . وطبعاً هذا له تأثير على الأمن القومي الليبي في جانبه الثقافي وحتى الاجتماعي والسياسي ، فلا أمن قومي بدون تأمين من الأمن السيبراني للدول التي ارتبطت بعالم الإنترنت .

من خلال ما تقدم يتضح بان الأمن السيبراني هو بحد ذاته وسيلة أمنية علمية الغرض منها هو حماية الأمن القومي وهو له دور في حماية جوانب الأمن القومي في النطاق او الفضاء السيبراني ؛ ولهذا فان العلاقة بين الاثنين انما هي علاقة تعاونية واحدة متشابكة لكون ان الأمن السيبراني هو أمن قومي ولكن نطاقه هو الفضاء الإلكتروني او السيبراني والجانب الآخر هناك نطاق تقليدي للأمن القومي تمثله اجهزة حكومية ملقى على عاتقها حماية جوانب الأمن القومي المختلفة ونطاقها غير سيبراني ، وتلك الاجهزة والمؤسسات مثل الأمن الداخلي والأمن الخارجي وادارة الضرائب والحرس البلدي والجمارك والجوازات والهجرة وجهاز الخدمات العامة او البيئة والقوات المسلحة وغيرها من المؤسسات التي تعنى بمصالح المواطنين ، وشخوصها ومعداتها الدفاعية تتحرك على الارض إضافة إلى نطاقها السيبراني ، أما الأمن السيبراني هو أمن قومي سيبراني نطاقه سيبراني وهو يقدم حمايته للأمن القومي سيبرانياً من خلال برامج وتطبيقات

إلكترونية عبر الإنترنت كالتشفير والتصدي للاختراقات ورسائل التصيد الإلكترونية والحماية من الفيروسات والتصدي للبرمجيات الضارة .

إذن مؤسسات حماية الأمن القومي التقليدية والتي تستخدم وسائل تقليدية للدفاع عن الأمن القومي تحتاج الى مؤسسة متخصصة لتحمي نطاقها السيبراني لصد الهجمات السيبرانية التي قد تتعرض لها وتهدد أمنها القومي سيبرانياً .

إذن هناك علاقة وثيقة بين الأمن السيبراني والأمن القومي فالأمن السيبراني هو وسيلة أمنية علمية للدفاع عن كافة جوانب الأمن القومي سيبرانياً .

ثانياً أهم التحديات التي تواجه تحقيق الأمن السيبراني .

الهجمات السيبرانية المختلفة التي تتعرض لها انظمة الحاسوب والشبكات والتطبيقات والبيانات والمعلومات المربوطة على الإنترنت من التحديات التي تواجه تحقيق الأمن السيبراني ، والهدف من هذه الهجمات هو استغلال غير مشروع لأنظمة الحواسيب والشبكات والمنظمات التي يعتمد عملها على تقنيات المعلومات والاتصالات الرقمية وذلك بإحداث أضرار او تعطيل او تشفير او ابتزاز ، والهجمات هذه تشمل كافة الانشطة الخبيثة التي هدفها الوصول غير المشروع او تدمير وسرقة البيانات والمعلومات للمستهدف بالهجمات السيبرانية مثل الهجمات الإلكترونية المتقدمة (APT) وهي تهديدات سيبرانية مستمرة وموجهة الهدف منها هو سرقة المعلومات أو التجسس . والهجمات السيبرانية اصبحت تتنوع وتتخصص وصارت من اهم التحديات التي تواجه الأمن السيبراني لكي يكون له دور في حماية الامن القومي . من ضمن التحديات التي تواجه تحقيق الأمن السيبراني كذلك هناك هجمات حجب الخدمة الموزعة والتي أشير بانها محاولات تقوم بها جهات عدائية لتعطيل الانظمة المختلفة من اجل انهاء خدمات تلك الأنظمة أي جعل خدماتها غير متوفرة وذلك بواسطة إرسال طلبات كثيرة من عدة مصادر في لحظة واحدة . إضافة إلى الهجمات السيبرانية يواجه الأمن السيبراني تحديات أخرى كعدم وعي بعض المستخدمين للأجهزة والتطبيقات والبرامج والشبكات المربوطة على الإنترنت وعدم توفر قوانين وتدابير

وقائية تجبر المستخدمين للفضاء السيبراني في بعض الدول على أخذ الاحتياطات الأمنية السيبرانية للحفاظ على بياناتهم ومعلوماتهم وتطبيقاتهم وبرامجهم وارشيفهم الإلكترونية وغيره . من خلال ما تقدم نجد ان الأمن السيبراني يواجه الكثير من التحديات والصعوبات لتحقيقه على ارض الواقع ليكون له دور في تحقيق الأمن القومي للدول ، فهو الوسيلة الأمنية العلمية الفنية التي تساهم في حماية كافة جوانب الأمن القومي في الفضاء الإلكترونية ، من أهم تلك التحديات إضافة إلى ما تقدم الأتي :-

1- **البرامج الخبيثة** :- تعد البرامج الخبيثة احد التحديات التي تواجه تحقيق الأمن السيبراني ليكون له دور في حماية الأمن القومي وخاصة البرامج التي اصداراتها حديثة فاختراق انظمة المؤسسات المالية والاقتصادية في ليبيا مثلاً والمربوطة على الشبكة الدولية للمعلومات الإنترنت وسرقة معلومات حساسة منها وتثبيت برامج خبيثة وفيروسات ضارة واتلاف ما في الاجهزة الالكترونية المربوطة على الانترنت من بيانات او سرقتها سوف يحدث خسائر واضرار اقتصادية تؤثر في الامن الاقتصادي الليبي والذي هو جانب مهم من جوانب الأمن القومي الليبي ولهذا فان توفر حماية ووقاية لتلك الانظمة من خلال التأمين السيبراني الذي يشكله الأمن السيبراني سوف يكون له دور في حماية الأمن القومي ، وعلى ذلك تعد البرامج الخبيثة خاصة المستحدثة والتي لم

يقاومها الأمن السيبراني من قبل وليس لديه أي معلومات وبيانات احد التحديات التي تواجه تحقيق الأمن السيبراني (57) .

فالبرامج الخبيثة خاصة ذات الإصدارات الحديثة تعد تحدي يواجه تحقيق الأمن سيبرانياً ، فقد اشير بان هجمات البرمجية الخبيثة و(اناسيري) (WannaCry) في مايو 2017 ، تسببت في تعطيل آلاف الأنظمة حول العالم، مما أدى إلى خسائر كبيرلعدد من الدول .

2- **خرق البيانات Equifax:** من التحديات تواجه الأمن السيبراني كذلك اختراق البيانات المدونة والمخزنة على الاجهزة الإلكترونية المربوطة على الإنترنت ، فقد واجهت الكثير من الدول مثل هذا التحدي على أمنها السيبراني فقد اشير بان من أحد أكبر الخروقات الأمنية على سبيل المثال هجمات ستواكسينت (Stuxnet) التي استهدفت البرنامج النووي الإيراني ، حيث تم سرقة بيانات شخصية لملايين الأشخاص (58) .

يعتبر الاختراق من أهم التحديات التي قد تواجه تحقيق الأمن السيبراني ليكون له دور في حماية الأمن القومي ، والاختراق هو قدرة الوصول الى البيانات والمعلومات بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص.

3- **برمجيات الفدية :** تعتبر من اهم مصطلحات الأمن السيبراني الحديثة وهي عبارة عن برمجيات ضارة تجعل بيانات وانظمة المستهدف بالهجوم غير قابلة للاستخدام وذلك الى حين دفع فدية مناسبة"(59) . وهذه البرمجيات تقوم بتشفير البيانات وتطلب فدية مقابل فك التشفير وهذا التحدي يواجه الأمن السيبراني حيث تواجه الكثير من الدول ومؤسساتها الخاصة والعامة والافراد هجمات سيبرانية مثل ما تعرضت له شركة مليتة النفطية عام 2024م ، والتي تعمل في مجال النفط في ليبيا إلى هجوم سيبرانياً قام بتنفيذه هاكوز عبر برنامج الفدية ، وقد زعم المصدر بان عملية الاختراق اسفر عن اخذ بيانات عن جوازات سفر وتأمين وتقارير جيولوجية وعن تفاصيل إنتاج الشركة النفطية ومراسلات سرية غاية في الأهمية ومعاملات مصرفية(60) .

هذا التحدي من التحديات التي تؤثر على الأمن القومي وهي تأتي إليه عبر الفضاء الإلكتروني وإدراك ومعرفة الأمن السيبراني يعد وقاية من أي هجوم سيبراني ، وكذلك عدم وجود معلومات عن هذا التحدي الذي يمثله برنامج الفدية لدى الأمن السيبراني يعد تحدي يهدد الأمن القومي إذا نجحت هجمات هذا البرنامج الى النفاذ الى خصوصيات الدولة وافرادها .

4- **التصيد الاحتيالي (Phishing)** :- يعتبر التصيد الاحتيالي من احد أهم التحديات التي تواجه تحقيق الأمن السيبراني ، وهو احد الوسائل الهجومية السيبرانية يتم عن طريق استخدام رسائل البريد الإلكتروني أو المواقع المزيفة لسرقة الهويات والبيانات الحساسة(61) .

والتصيد الاحتيالي يتم من خلال رسائل التصيد الإلكتروني وقد عرف بانه " التنكر على هيئة جهة جديرة بالثقة. ومن ثم إرسال رسائل بريد إلكتروني للحصول على معلومات حساسة. مثل : أسماء المستخدمين ، كلمات المرور ، تفاصيل بطاقات الائتمان ، وغيرها . وذلك من أجل نوايا خبيثة وسلبي"(62).

5- **عدم وجود وعي سيبراني** :- الكثير من الدول خاصة النامية لا تعي اهمية الأمن السيبراني كالدولة الليبية ، والدليل على ذلك عدم إصدار قانون للأمن السيبراني او تأسيس مؤسسة تعنى بالأمن السيبراني الذي صار ضرورياً مع التطور السريع في وسائل الاتصال عبر شبكات الإنترنت وكثرة الهجمات السيبرانية واستخدامها بدل الحروب التقليدية والتي صارت تهدد الأمن القومي ،إضافة إلى أهمية الأمن السيبراني في حماية الأمن القومي خاصة السيبراني .

6- **عدم وجود وعي جماهيري على نطاق واسع بالأمن السيبراني** الامر الذي يعد تحدي يواجه تحقيق الأمن السيبراني ليكون له دور في حماية الأمن القومي سيبرانياً خاصة في الدول النامية مثل ليبيا .

7- **عدم وجود مؤسسة حقيقية متخصصة تعنى بالأمن السيبراني** : هناك الكثير من الدول ليس لديها مؤسسة حقيقية متخصصة في الأمن السيبراني مثل ليبيا تدار من خلال متخصصين في الأمن والأمن السيبراني وفي أمن المعلومات ومتخصصين في تكنولوجيا المعلومات والاتصالات .

8- **سوء استخدام التقنية في مجال الوسائل المربوطة على الإنترنت** .

9- **عدم كفاءة بعض المستخدمين للفضاء الإلكتروني** خاصة في المؤسسات العامة التي تهديدها يعنى تهديد الأمن القومي بكافة جوانبه ، وما حدث في ليبيا من اختراقات للبيانات لشركة مليتة عام2024 لخير دليل .

10- **عدم وجود قانون للأمن السيبراني** : هناك الكثير من الدول لم تصدر قانون متخصص وصريح هدفه حماية الأمن القومي وصد الهجمات السيبرانية بالأمن السيبراني من تلك الدول على

سبيل المثال ليبيا رغم ان ليبيا قد اصدرت قانون مكافحة الجرائم الإلكترونية الذي هو في حد ذات قانون يمكن ان يضم الى قانون العقوبات الليبية وليس بمكانة وأهمية القانون السيبراني .

10- **الفيروسات الحاسوبية :** نوع من البرامج تهاجم الحواسيب بهدف التخريب حيث أنها تلحق الضرر بنظام المعلومات او البيانات وهذه البرنامج يعد من التحديات التي تواجه الأمن السيبراني خاصة في الدول النامية البعيدة عن ثقافة الأمن السيبراني وخاصة البرامج الحديثة من هذا النوع ، ولهذا فان هذا التحدي يساهم في تهديد الأمن القومي سيبرانياً . الفقرة الرابعة من المادة الاولى من القانون رقم 5 لسنة 2022م . بشأن مكافحة الجرائم الالكترونية ، بنغازي– ليبيا .

11- **البرمجيات الضارة :** هي نوع من البرامج التي تستخدم لغرض انتهاك سرية او سلامة او توفير بيانات الأنظمة الإلكترونية او تطبيقاتها او أنظمة التشغيل الخاصة بتلك الأنظمة ، وهذه البرمجيات تعد من التحديات التي تواجه الأمن السيبراني (63) .

ثالثاً الحلول والمعالجات لتحقيق الأمن السيبراني :

من الحلول والمعالجات لتحقيق الامن السيبراني نذكر الاتي :-

1- منع الهجمات السيبرانية من خلال عدد من السياسات والضوابط حيث ذكرت الدراسات المتخصصة في الأمن السيبراني ذلك حيث تقول دراسة ذاكرة تلك التدابير :- " تشمل هذه التدابير في الأمن السيبراني بناء سياسات وضوابط وأنظمة مثل إنشاء جدران الحماية وبرامج مكافحة الفيروسات وأنظمة كشف التسلل والوقاية منها والتشفير وكلمات المرور في عمليات تسجيل الدخول" (64) .

2- التعاون بين القطاع العام والخاص في المجال السيبراني لتحسين الأمن السيبراني .

3- ضرورة التأكد بأن الأجهزة المرتبطة على الإنترنت تستعمل أحدث البرامج وأحدث الاصلاحات الأمنية .

وكانت من ضمن السياسات الامنية السيبرانية الامريكية ان اصدرت وزارة الدفاع في عام 2011م دليلاً يسمى (استراتيجية وزارة الدفاع للعمل في الفضاء السيبراني) والذي اشير بانه حدد خمسة اهداف وهي وكما ذكرها المصدر :-

" أ- التعامل مع الفضاء الإلكتروني كمجال تشغيلي .

ب- استخدام مفاهيم دفاعية جديدة لحماية شبكات وأنظمة وزارة الدفاع.

ج- الشراكة مع وكالات أخرى والقطاع الخاص.

د- السعي إلى تطبيق استراتيجية الأمن السيبراني للحكومة بأكملها .

ر- العمل مع الحلفاء الدوليين لدعم الأمن السيبراني الجماعي ودعم تطوير القوى العاملة السيبرانية القادرة على الابتكار التقني السريع "(65) .

4- الوقاية من الهجمات السيبرانية من خلال تأمين الأجهزة الإلكترونية والشبكة الدولية للمعلومات الإنترنت حيث أكد ذلك الكثير من المتخصصين في مجال الامن السيبراني (66) .

5- وقاية شبكات واجهزة الدولة الإلكترونية وذلك من خلال وضع برامج حماية من اي هجمات سيبرانية التي قد تحدث من خلال اختراقات خارجية تضر بكافة جوانب الأمن القومي للدولة .

6- اقامة ورش العمل والندوات والمؤتمرات للتعريف والتثقيف بالأمن السيبراني .

7- ضرورة نشر الوعي الثقافي بأهمية الأمن السيبراني على نطاق واسع يشمل الافراد والمؤسسات وفي هذا الخصوص فقد رات دراسة بضرورة تحفيز ثقافة وطنية للأمن السيبراني . كما ذكرت الدراسة بالقول :- " أن نقطة انطلاق الأمن السيبراني الوطني تبدأ بتطوير سياسة وطنية لرفع الوعي حول قضايا الأمن السيبراني والحاجة لإجراءات وطنية والى التعاون الدولي" (67) .

8- تشكيل فريق امني متخصص بتكنولوجيا المعلومات وظيفته تقديم المساعدة للمؤسسات الحكومية وغير الحكومية لتأمين اجهزتها وشبكاتها الإلكترونية والمربوطة على الإنترنت للحد والوقاية من الهجمات السيبرانية ، وكذلك حماية اصولها الحساسة المتواجدة بملفاتها الإلكترونية ، وبهذا الخصوص فقد قامت الكثير من الدول بتأسيس مراكز الاستجابة لطوارئ الكمبيوتر (CERT)(68) .

9- ضرورة حماية البنية التحتية التي تمر خلالها اسلاك الشبكة الإلكترونية .

10- ضرورة تأمين الشبكات الإلكترونية من أي هجمات سيبرانية .

11- ضرورة مرقبة الإنترنت والأجهزة الإلكترونية وحمايتها من أي اختراق سيبراني .

12- ضرورة تأمين السحابة الالكترونية.

13- ضرورة تأمين التطبيقات الالكترونية(69) .

14- ضرورة تعلم لغات البرمجيات المهمة للأمن السيبراني مثل بيثون (Python) و++c ، جافا (Java) ، روبي (Ruby) .

15- ضرورة دراسة وتعلم اساسيات الشبكات مثل (Tcp/ip) و (Dns) و(Dhcp) و(http) و(https) و(Tls) و(ssl)(70) .

16- تشجيع المخترعين في مجال نظم المعلومات والبيانات من اجل مساندة الأمن السيبراني للدولة فعلى سبيل المثال جاء في فقرة من فقرات المادة (35) من القانون رقم (5.20) بشأن الامن السيبراني المغربي والذي وضع من قبل خبراء في الأمن السيبراني بعد دراسة وتدقيق ، تقول تلك الفقرة :- "تشجيع البحث والتطوير في مجال الأمن السيبراني "

17- ضرورة ان تجبر الدولة المؤسسات العامة والخاصة بوضع تدابير واجراءات لحماية انظمتها ومعلوماتها من الهجمات السيبرانية . وفي هذا الصدد يقول بروس شنير (Bruce Schneier) مؤسس شركة «كوبرتينو» لأمن الإنترنت، أن الشركات لن تقوم بعمل إستثمارات كافية في مجال الأمن السيبراني ما لم تجبرها الحكومة على القيام بذلك. ويذكر أيضاً أن الهجمات الإلكترونية الناجحة على الأنظمة الحكومية لا تزال تحدث رغم الجهود الحكومية(71) .

18- حماية الأنظمة الأساسية لمجال الأمن السيبراني كأجهزة الحاسوب والاجهزة الذكية المختلفة والشبكات الإلكترونية والسحابة الإلكترونية لتخزين البيانات .

19- ضرورة استحداث وظائف جديدة في كافة المؤسسات الحكومية وغير الحكومية في الملاك الوظيفي تحت مسمى موظف الأمن السيبراني من مهامه متابعة ومراقبة جوانب الأمن السيبراني المختلفة وتقييم اداء للتقنيات والمخاطر والثغرات للبيئات التقنية . وكذلك تطوير ادوات الدفاع

السيبراني ووصف تحليل حركة المرور على الشبكة الإلكترونية وتحديد الانشطة المعادية والشاذة التي تهدد البيانات والشبكة والانظمة الإلكترونية .

20- تشفير وسائط التخزين الخاصة بالأجهزة الإلكترونية المربوطة على الإنترنت خاصة التي تحوي بيانات ومعلومات حساسة وفقاً لمعيار التشفير المعتمد .

21- ضرورة منع استخدام وسائط التخزين الخارجية .

22- ضرورة الحصول على اذن من الجهة المعنية بالأمن السيبراني بشان امتلاك استخدام وسائط التخزين الخارجية .وأن تحمل مؤسسات الدولة مسؤولية تأمين البيانات للحفاظ عليها وحمايتها من أي هجمات سيبرانية حفاظاً على الأمن القومي(72) .

23- ضرورة تأسيس مؤسسة تعنى بالأمن السيبراني ففي قوانين الأمن السيبراني في الدول التي تعي اهمية هذا الأمن نجد الإيعاز بتأسيس لجنة لاستراتيجية الأمن السيبراني حيث نجد ذلك على سبيل المثال في القانون السيبراني للمملكة المغربية فقد نصت عليه المادة (35) من القانون والتي تقول :- " تحدث لجنة استراتيجية للأمن السيبراني ، يعهد اليها بالقيام بكل يلي :-

- إعداد التوجهات الاستراتيجية للدولة في مجال الأمن السيبراني والسهر على ضمان صمود نظام معلومات الهيئات والبنيات التحتية ذات الاهمية الحيوية والمتعهدين المشار اليهم في الفرع الثالث من الفصل الثاني من هذا القانون .

- التقييم السنوي لأنشطة السلطة الوطنية .

- تقييم عمل اللجنة الوطنية لإدارة الازمات والاحداث السيبرانية الجسيمة . المنصوص عليها في المادة(36) وما بعده .

- حصر نطاق افتحاصات امن نظم المعلومات التي تنجزها السلطة الوطنية .

- تشجيع البحث والتطوير في مجال الأمن السيبراني .

- تشجيع برامج وانشطة التحسيس وتعزيز القدرات في مجال الأمن السيبراني لفائدة الهيئات والبنيات التحتية ذات الاهمية الحيوية ؛

- إبداء الرأي في مشاريع القوانين والنصوص التنظيمية المتعلقة بمجال الأمن السيبراني.

يحدد بنص تنظيمي تأليف وكيفيات سير اللجنة الاستراتيجية للأمن السيبراني . " (73) .

24- كما يتطلب ان تقوم الحكومات بإصدار تدابير ولوائح وتوجيهات متخصصة لحماية تقنية المعلومات وانظمة الحواسيب موجهة الى مؤسساتها بشأن اخذ الاحتياطات الامنية السيبرانية

واجبارها على حماية انظمتها ومعلوماتها وبياناتها من الهجمات السيبرانية التي تكون على هيئة فيروسات وديدان واحصنة طروادة والتصيد وهجمات رفض Dos والوصول غير المصرح به وغيره (74) .

وقد اتخذت عدد من الدول المتقدمة مثل هذه التدابير والاجراءات فعلى سبيل المثال في مارس من عام 2011 حدد تقرير مكتب محاسبة الحكومة الامريكية حماية انظمة معلومات الحكومة الفيدرالية والبنية التحتية للإنترنت كمنطقة وعنصر بالغ الخطورة في نطاق الحكومة . ومع بروز الهجمات السيبرانية والخطر الذي صار يحدق بالفضاء السيبراني للولايات المتحدة الامريكية اصدرت وزارة الدفاع الامريكية في نوفمبر 2013م قاعدة ونظام الأمن السيبراني جديد وهو (Fed.Reg.6937378) حيث فرض النظام الجديد عدد من المتطلبات على المقاولين كاتباع معايير Nist (IT) والالتزام بالإبلاغ عن أي خروقات او هجمات سيبرانية لوزارة الدفاع (75) .

25- ضرورة ان تقوم الدول بإصدار قوانين تخص الأمن السيبراني تضع فيها سياساتها في الأمن السيبراني فلو نظر إلى قانون أمن المعلومات الفيدرالي الصادر عام 2002م الذي يخص الولايات المتحدة الامريكية نجده من ضمن احد القوانين الاساسية التي تحكم انظمة الأمن السيبراني

الفيدرالية في الولايات المتحدة الامريكية ، اضافة الى خطوات وسياسات اخرى في الأمن السيبراني فعلى سبيل المثال في سبيل تأمين الفضاء السيبراني للولايات المتحدة الامريكية قام الكونغرس الأمريكي عام 2004م بتخصص ٤.7 مليار دولار لتأمين الفضاء الإلكتروني . كما اشير بان الأمن السيبراني شرط اساسي لحماية الفضاء السيبراني للدول حيث اشير بانه شرط اساسي للأمن السيبراني الهندي فقد اشير بان شركة (انتريكس) قد ذكرت بان الخبير في مجال الإنترنت ومحامي المحكمة العليا الهندية بافان دوغال (Pavan Duggal) قال في خصوص الأمن السيبراني :- " التشريعات المخصصة لأمان الإنترنت هو شرط أساسي في الهند ، ولا يكفي مجرد وضع سياسات الأمن السيبراني كجزء من قانون تقنية المعلومات . علينا أن نرى الأمن السيبراني ليس فقط من منظور قطاعي ، ولكن أيضا من منظور وطني " (76) .

26- ضرورة وضع سياسات وضوابط وانظمة لتأمين الأمن السيبراني كإنشاء جدران الحماية وبرامج مكافحة الفيروسات وانظمة كشف التسلل والوقاية منها والتشفير وكلمات المرور في عمليات الدخول(77) .

27- التنسيق بين المؤسسات الحكومية وغير الحكومية المحلية والاقليمية والدولية من اجل المن السيبراني فقد اكدت دراسة بشأن الأمن السيبراني بضرورة التنسيق مع الاجهزة الأمنية

المتخصصة والمؤسسات العامة ومع المنظمات الغير حكومية المحلية العربية كجمعيات التكنولوجيا والاتصالات المرصد العربي لأمن وسلامة الفضاء السيبراني، والاقليمية كالشبكة العربية لهيئات تنظيم الاتصالات الدولية كالاتحاد الدولي للاتصالات والشبكة الاورو- متوسطية لمنظمي الاتصالات(78) .

28- ضرورة وضع مستويات دفاعية متعددة من الضوابط والاجراءات الأمنية المختلفة عن طريق التكامل بين الاشخاص والتقنيات والقدرات التشغيلية المتنوعة .

29- ضرورة ان تكون هناك معلومات استباقية للتهديدات من خلال مجموعة من المعلومات المنظمة قد تم تحليلها حول الهجمات السيبرانية الاخيرة والحالية والمحتملة والتي بالإمكان ان تشكل تهديد سيبراني.

30- ضرورة ان يكون هناك تبادل في البيانات والمعلومات والمعرفة لغرض استعمالها في إدارة المخاطر والتهديدات او الاستجابة للأحداث السيبرانية وذلك ضمن عملية مشاركة المعلومات .

31- ضرورة توفير حماية عن طريق برمجيات تحد من حركة مرور بيانات الشبكات من خلال ما يسمى جدار الحماية وذلك وفق لعدد من قواعد تمكين الوصول والتي تحكم ما هو مسموح ومصرح به من عدمه(79) .

رابعاً النتائج والتوصيات :

مع هذا التطور السريع في وسائل الاتصال وعالم الإنترنت واعتماد مؤسسات القطاع العام والخاص والافراد على الإنترنت في الاطلاع والتواصل والارشفة صار من الضروري ان يتم وضع استراتيجية من اجل توفير أمن سيبراني لحماية خصوصيات المؤسسات والافراد ويكون له دور في حماية الأمن القومي .
واحتياطات الأمن السيبراني حساسة وحساسة جدا ؛ لأن أي خطأ قد يتحول إلى هزيمة سيبرانية بدل من النصر بمعنى ان تكون الاحتياطات الأمنية السيبرانية لحماية أمنها السيبراني دقيقة ؛ لان الخطأ في تنفيذ الاحتياطات يؤدي الى مشكلة وضرر بالفضاء السيبراني للدولة المعتدى عليها ولهذا صارت الدول تتخذ سياسات من اجل تأمين فضاءها السيبراني من أي اعتداءات وهجمات سيبرانية متوقعة من خلال وضع القوانين المتعلقة بالأمن السيبراني . في ليبيا لم يصدر قانون متعلق بالأمن السيبراني انما صدر قانون بشان الجرائم الإلكترونية وهو القانون رقم 5 لسنة 2022 م بشأن مكافحة الجرائم الإلكترونية والذي يعتبر جزء من قانون العقوبات المعمول بها في ليبيا . من خلال ما تقدم من الدراسة برزت عدد من النتائج والتوصيات .

أ- النتائج :

اضافة الى ما ظهر من تحديات تواجه الامن السيبراني فقد اتضحت النتائج التالية :-

1- إن للأمن السيبراني دور في حماية الأمن القومي .

2- عدم وجود قانون متعلق بالأمن السيبراني في بعض الدول مثل ليبيا ليكون له دور في حماية أمنها القومي من الهجمات السيبرانية .

3- إن الأمن السيبراني جزء من الأمن القومي .

4- عدم وعي وكفاءة المستخدمين للأجهزة المربوطة على الإنترنت بخطورة الهجمات السيبرانية.

5- الكثير من العاملين الذين يتعاملون مع الشبكة الدولية للمعلومات في مؤسسات الدول سواء كانت عامة أوخاصة ليس مؤهلين لمثل هذا العمل الخطير.

6- وجود تحديات تهدد الأمن السيبراني تمثلها عدة انواع من الهجمات السيبرانية .

7- عدم مواكبة التطور في مجال المعلومات والاتصالات لبعض الدول مما يهدد الأمن السيبراني .

8- عدم وجود اجهزة ومكاتب لبعض الدول والتي من بينها ليبيا لحماية الفضاء الإلكتروني الخاص بها من أي هجمات سيبرانية.

9- عدم شفافية المؤسسات التي تتعرض لهجمات سيبرانية من الإعلان عنها .

10-سوء استخدام التقنية في مجال الوسائل المربوطة على الإنترنت .

ب- توصيات :

1- ضرورة فتح اقسام وفروع في المؤسسات التعليمية سواء كانت مدنية او عسكرية تهتم بتدريس الأمن السيبراني من اجل تخريج جيل من المتخصصين في الأمن السيبراني ليكونوا جنود لصد الهجمات السيبرانية ومنع أي اختراقات لشبكات الاتصال في الدولة .

2- ضرورة ان يكون هناك اطلاع مستمر ويومي لما يحدث في العالم من تقدم تكنولوجي في وسائل الاتصال والتكنولوجيا من قبل مستخدمي الإنترنت موطني ومؤسسات والذين يعتمدون على تخزين بياناتهم الشخصية على الاجهزة المرتبطة بالإنترنت .

3- التعاون مع الدول المتقدمة في مجال تبادل المعلومات والاكتشافات والاختراعات في مجال الاتصالات والمعلومات من خلال اتفاقيات اقليمية ودولية.

4- على الدول التي لم تصدر قوانين صريحة تخص الأمن السيبراني أن تقوم بإصدارها مثل الدولة الليبية ليكون لها دور في حماية الأمن القومي .

5- أن تكون هناك قاعدة بيانات احتياطية وتأمينها ببرامج استرداد حديثة .

6- ضرورة استحداث مؤسسة تعنى بالأمن السيبراني للدول التي ليس لديها مثل تلك المؤسسة كالدولة الليبية.

7- ضرورة خلق قدرات وطنية لإدارة حوادث الحاسب الآلي.

8- ضرورة وقاية شبكات واجهزة الدولة الإلكترونية من أي هجمات سيبرانية تضر بكافة جوانب الأمن القومي للدولة .

9- تشجيع المخترعين في مجال نظم المعلومات والبيانات من اجل مساندة الامن السيبراني للدولة .

10- إقامة ورش العمل والندوات والمؤتمر للتعريف بما يستجد في عالم التكنولوجيا والمعلومات والاتصالات والأمن السيبراني ،

11- تشجيع على تعلم الأمن السيبراني .

12- ضرورة ان تقوم المؤسسات العامة والخاصة بوضع تدابير واجراءات لحماية انظمتها ومعلوماتها من الهجمات السيبرانية من خلال قانون ملزم .

13- ضرورة تطوير وتبني تقنيات أمنية للتصدي للهجمات السيبرانية.

14- التكيف مع البيئة الخارجية الجديدة وتحديث وسائل أمنية سيبرانية لصد الهجمات السيبرانية المختلفة .

15- نشر الوعي الأمني السيبراني بين المواطنين والمؤسسات الحكومية وغير الحكومية من خلال وسائل التنشئة الاجتماعية والسياسية والثقافية .

16- ضرورة ان تكون هناك شفافية من قبل المؤسسات التي تتعرض لهجمات سيبرانية بان تعلن عنها وعن مصدرها لتساعد القائمين على الأمن السيبراني في إيجاد الحلول .

الهوامش والمراجع

1- على الموقع https://mofeeed.com/the-origin-of-the-word-cyber. تاريخ. الاطلاع علية 2024/4/15.

2- على الموقع https:/mofeed.com/the-best-saudi-universties-to- study- cyberecurity. تاريخ الاطلاع عليه 2024/4/20.

3- " سايبر" ، https://ar.wikipedia.org. تاريخ الاطلاع عليه 2024/4/11.

4- " تاريخ_الأمن_السيبراني " . 2021/11/17. https://mawdoo3.com . تاريخ الاطلاع عليه 2024/4/17.

5- على الموقع https://mofeeed.com/the-origin-of-the-word-cyber . مرجع سابق.

6- على الموقع . https://www.ncsc.gov.bh › cyberwiser › cyber-security . تاريخ الاطلاع عليه 2024/5/3.

7- المرجع السابق .

8- "المفاهيم-الإدارية. الأمن-السيبراني" . ...https://hbrarabic.c om . تاريخ الاطلاع عليه 2024/4/20.

9- على الموقع .https://mofeeed.com/the-origin-of-the-word-cyber .
مرجع سابق .

10- على الموقع . https:/mofeed.com/the-best-saudi-universties-to-study-cyberecurity. مرجع سابق .

11- على الموقع .https://studyfans.com › blogs › what-is-the-difference-be. تاريخ الاطلاع عليه 2024/4/18.

12- "ما هوالهاكر الاخلاقي ؟ - العلاقة بين الهاكينج الاخلاقي والامن السيبراني" . 2023/8/9 . https://ae.linkedin.com › pulse . تاريخ الاطلاع عليه 2024/4/22.

13- القانون رقم 5.20 المتعلق بالأمن السيبراني. المادة (2) ، الجريدة الرسمية العدد 6904 ، 2020/7/30 ، تطوان -المغرب .

14- "ما المقصود بالأمن السيبراني" ، › https://aws.amazon.com › what-is
cybersecurity . تاريخ الاطلاع عليه 2024/4/15 .

15- المرجع السابق .

16- على الموقع .- https://cisca.com/c/ar-ae/products/security/what .
is-cybersecurity.html. تاريخ الاطلاع عليه 2024/4/11 .

17- "ما هو الامن السيبراني" . https://www.ejaba.com › question . تاريخ الاطلاع عليه 2024/4/15 .

18- على الموقع https://www.alnwrsraby.com . تاريخ الاطلاع عليه 2024/5/7 .

19- على الوقع . http://www.tra.gov.lb/Cybersecurity .. تاريخ الاطلاع عليه 2024/4/12 .

20- "فوائد الامن السيبراني" . 2023/1/15 .
https://bakkah.com › knowledge-center . تاريخ الاطلاع عليه 2024/5/2 .

21- "تقنية معلومات" . 2023/6/25 . https://a8laam.com. تاريخ الاطلاع عليه 2024/4/2.

22- المرجع السابق .

23- على الموقع https;//bluemediasa.com/cyber-security . تاريخ الاطلاع عليه 2024/4/18.

24- المرجع السابق .

25-على الموقع https://nordvpn.com › cybersecurity . تاريخ الاطلاع عليه 2024/4/20.

26- بن عبد الرازق ، حنان ، (2017/2016)، تأثير المأزق الأمني الاثني على الاستقرار الداخلي للدولة – دراسة للنموذج الاسباني 1936 ، (رسالة دكتوراه ، كلية الحقوق والعلوم السياسية والعلاقات الدولية ، جامعة محمد خضير ، بسكرة - الجزائر)، ص26.

27- موسى، ذياب البدانية. (2009) . الامن الوطني في عصر العولمة. (الرياض –الاسكندرية) : مؤسسة شباب الجامعة .ص24.

28- هويدي ، أمين . (1975) . الأمن العربي في مواجهة الأمن الإسرائيلي .(ط1) . (بيروت – لبنان): دار الطليعة للطباعة والنشر .ص42 .

29- القانون رقم (4) بإنشاء مجلس الامن الوطني المادة (2) . (2007/1/22) . انشاء مجلس الامن الوطني ، مؤتمر الشعب العام .سرت. المادة 2 .

30- نافع ، محمد عبدالكريم ،(1975) ، الأمن القومي الجزء الأول .(ط1) . (القاهرة –مصر): مطبعة الشعب .ص65 .

31- طاهر، علاء (يناير1986) . نظرية الأمن القومي الإسرائيلي، مجلة الوحدة. العدد (23) . الرباط –المغرب : المجلس القومي للثقافة . ص35 .

32- علام ، أشرف . (2008) . مشروع قناة البحرين والأمن العربي .(القاهرة –مصر) : مجموعة النيل العربية .ص16 .

33- سالم ، محمد صلاح . (2003) . العراق ماذا جرى ؟ . . واحتمالات المستقبل . (ط1) . (القاهرة– مصر) : عين للدراسات والبحوث الإنسانية والاجتماعية ، ص ، ص135،134 .

34- المرجع السابق ، ص135 .

35- خشيم ، مصطفى عبد الله . (1995) . موسوعة علم العلاقات الدولية . (ط1)

.(طرابلس- ليبيا) : الدار الجماهيرية لنشر والتوزيع والإعلان.ص53.

36- فوزي ، محمد ،(1983) حرب الثلاث سنوات . (ط2). (بيروت- لبنان) : دار الوحدة.ص18.

37- بن عبد الرازق، حنان ، مرجع سابق ، ص17 .

38- المرجع السابق ، ص18.

39- هويدي ، امين . (1991) . العسكرة والأمن في الشرق الأوسط : تأثيرها على التنمية والدمقراطية . (القاهرة – مصر) : دار الشروق .ص52.

40- عبد المهدي ، محمد عشري حسن ، (2014) ، الاستقرار الامني وأثره على التنمية الاقتصادية في مصر : ظاهرة الأمنوتنموية . Http://search.mandumah.com/Record/687322 .تاريخ الاطلاع عليه 2024/4/2.

41- مسعود ،عبد الله محمد و مراد ،علي عباس ،(2006) ، الأمن والأمن القومي .(ط1). (بنغازي ، ليبيا) : المركز دراسات الكتّاب الاخضر، ص70 .

42- علام ، اشرف ، مرجع سابق ، ص 89 .

43- سالم ،محمد صلاح ، مرجع سابق ، ص138.

44- مسعود ، عبد الله محمد ، مراد علي عباس ، مرجع سابق ، ص80.

45- المرجع السابق ، ص83.

46- بن عبد الرازق، حنان ، مرجع سابق ، ص39 .

47- محمد ،ابراهيم عبد القادر.(2013/2012) . التحديات الداخلية والخارجية المؤثرة على الامن الوطني الاردني في الفترة 1999- 2013 دراسة حالة. (رسالة ماجستير. كلية الآداب والعلوم . جامعة الشرق الاوسط . الاردن) ، https://meu.edu.jo › libraryTheses . تاريخ الاطلاع عليه 2024/4/11.

48- المرجع السابق .

49- على الموقع http://www.tra.gov.lb/Cybersecurity-in-few-words-AR تاريخ الاطلاع عليه 2024/5/12

50- الصلج ، نوال ، 9-2021/11/18 . المخدرات الرقمية على المجتمعات العربية. من أعمال المؤتمر الدولي الأول حول المخدرات والمؤثرات العقلية ، طرابلس –ليبيا .

51- المرجع السابق ، ص129 .

52- المرجع السابق ، ص123 .

53- المرجع السابق ، ص122 .

54- نور الدين ، بم سولة ، الزهرة ، جبر ،9-18/11/2021 . المخدرات الإلكترونية ، من أعمال المؤتمر الدولي الأول حول المخدرات والمؤثرات العقلية ، المرجع السابق ، ص164 .

55- على الموقع . http://www.tra.gov.lb/SubPagear.aspx?pageid=3239. تاريخ الاطلاع عليه 2024/4/12 .

56- المرجع السابق .

57- على الموقع . https://www.secprint.sa › cyber-attacks . تاريخ الاطلاع عليه 2024/4/11 .

58- على الموقع . https://bluemediasa.com/cyber-security . مرجع سابق .

59- على الموقع . 2022/3/22 . . https://mofeeed.com/cyper-security-words . تاريخ الاطلاع عليه 2024/5/3 .

60- "برامج هنا الحدث " 2024/5/4، قناة ليبيا الحدث ، على الموقع www. Libya Alhadath.

61- على الموقع .https://bluemediasa.com/cyber-security . مرجع سابق .

62- على الموقع .https://mofeeed.com/cyper-security-words . مرجع سابق.

63- المرجع السابق.

64- قوانين الامن الالكتروني ، ويكيبيديا ، الموسوعة الحرة https://ar.wikipedia.org/wiki . تاريخ الاطلاع عليه 2024/4/11.

65- المرجع السابق .

66- المرجع السابق.

67- "حماية الاطفال والمستهلكين على شبكة الانترنت" .http://www.tra.gov.lb/Cybersecurity-in-few-words-A. تاريخ الاطلاع عليه 2024/4/19.

68-   على الموقع

. http://www.tra.gov.lb/SubPagear.aspx?pageid=3240 .   . تاريخ

الاطلاع عليه 2024/4/21 .

69-   ـ على الموقع . https://nordvpn.com › cybersecurit) .مرجع سابق .

70-   على الموقع . 2023 . https://academy.hsoub.com › questions . تاريخ

الاطلاع عليه 2024/5/3 .

71-   قوانين الأمن الالكتروني، مرجع سابق .

72-   "ما المقصود بالأمن السيبراني" . مرجع سابق .

73-   القانون 5-20 لسنة 2020 المتعلق بالأمن السيبراني ، المادة (35) . مرجع سابق .

74-   قوانين الأمن الالكتروني، مرجع سابق .

75-   المرجع السابق .

76-   المرجع السابق.

77-   المرجع السابق .

78-على   الموقع   .

تاريخ الاطلاع   .http://www.tra.gov.lb/SubPagear.aspx?pageid=3238

.2024/4/4

79-على الموقع .   https://mofeeed.com/cyper-security-words .مرجع

سابق.

فهرس المحتويات